Golden

MATHS SERIES

MODERN ALGEBRA

Published by :
LAXMI PUBLICATIONS (P) LTD.
22, Golden House, Daryaganj,
New Delhi-110002.

Phones : **011-23 26 23 68**
011-23 26 23 70

Faxes : **011-23 25 25 72**
011-23 26 22 79

Branches :
- 129/1, IIIrd Main Road, IX Cross, Chamrajpet, **Bangalore** (*Phone* : 080-26 61 15 61)
- 26, Damodaran Street, T. Nagar, **Chennai** (*Phone* : 044-24 34 47 26)
- St. Benedict's Road, **Cochin** (*Phone* : 0484-239 70 04)
- Pan Bazar, Rani Bari, **Guwahati** (*Phones* : 0361-254 36 69, 251 38 81)
- 4-2-453, 1st Floor, Ramkote, **Hyderabad** (*Phone* : 040-24 75 02 47)
- Adda Tanda Chowk, N.D. 365, **Jalandhar City** (*Phone* : 0181-222 12 72)
- 106/A, Ist Floor, S.N. Banerjee Road, **Kolkata** (*Phones* : 033-22 27 37 73, 22 27 52 47)
- 18, Madan Mohan Malviya Marg, **Lucknow** (*Phone* : 0522-220 95 78)
- 128A, Block 3, First Floor, Noorani Building, L.J. Road, **Mumbai** (*Phone* : 022-24 46 39 98)
- Radha Govind Street, Tharpagna, **Ranchi** (*Phone* : 0651-230 77 64)

EMAIL : colaxmi@hotmail.com

WEBSITE : www.laxmipublications.com

ISBN 81-7008-045-2

MGA-6711-040-G. MODERN ALGEBRA (C)

Price : **Rs. 40.00** *Only*

C—10424/05/05

Laser Typesetting at :

Printed at : Mehra Offset Press, New Delhi

CONTENTS

1

Introduction

Before we start with Modern Algebra, we require the working knowledge of **Set-Theory, Mappings, Binary Operations, Number System** ; etc. Let us take one by one.

SECTION—A
SET-THEORY

Definitions :

1. Set. *It is a collection of definite and distinct objects of our preception or thought.*

The set is usually denoted by the capital letters of the alphabet, *viz.*, A, B, C, X, Y, Z ; etc.

For Ex. (I) Colleges affiliated to G.N.D. University.

(II) States of India.

(III) Points on a st. line.

2. Elements. *The objects which form the set are known as elements of the set.*

The elements are usually denoted by the small letters of the alphabet ; *viz.* a, b, c, x, y, z ; etc.

For Ex. In above (I), *colleges* are elements of the set.

In above (II), *states* are elements of the set.

In above (III), *points* are elements of the set.

Symbols : (I) $\in$ means '*belongs to*' or '*is an element of*' or '*is a member of*'.

(II) $\notin$ means '*does not belong to*' or '*is not an element of*' or '*is not a member of*'.

3. Finite and Infinite Sets.

(*i*) *A set is said to be* **finite** *if it has finite number of elements.*

For Ex. (I) The set of districts in Punjab.

(II) The set of numbers 2, 4, 6, 8.

(*ii*) *A set is said to be infinite if it has infinite number of elements.*

For Ex. (I) The set of points on a st. line.

(II) The set of st. lines in a plane.

4. Representation of a Set.

There are two methods to represent a set.

(*i*) **Roaster or Tabular Form.**

In this case *the set is denoted by listing all its elements, separating the elements by commas and enclose them in curvilinear brackets* { }.

For Ex. The set of numbers 2, 4, 6, 8 is written as

$$\{2, 4, 6, 8\}.$$

(*ii*) **Builder Form.**

In this case *the set is denoted by specifying the defining property.*

Thus the set S is denoted as $S=\{x \mid P(x)\}$.

Here x stands for '*a particular element of the set*' and the symbol (|) stands for '*such that*'.

For Ex. The set of numbers 2, 4, 6, 8 is written as

$$\{x \mid x \text{ is one-digited even positive integer}\}.$$

☞ **Cautions : I. The order of elements is immaterial in a set.**

Thus {2, 4, 6, 8}, {4, 6, 8, 2}, {6, 8, 2, 4} represent the same set.

II. Repetition of elements is not allowed in a set.

Thus {2, 4, 4, 6, 8}, {2, 4, 4, 4, 6, 6, 8} represent the same set {2, 4, 6, 8}.

5. Null Set. *A set having no element is called a null set.*

This is also known as **empty set** or **void set** and is denoted by ϕ.

For Ex. (I) Set of male students in a Women College.

(II) $\phi=\{x \mid x \text{ is an integer and } x^2=3\}$.

6. Singleton. *A set having only one element is called a* **singleton.**

This is also known as **unit set** or **one-point set.**

For Ex. (I) Set of Lady Prime Ministers of India.

(II) Set {3}.

☞ **Caution :** ϕ and $\{\phi\}$ do not represent the same set because ϕ is a null set while $\{\phi\}$ is a singleton.

7. Equality of Sets

Two sets are said to be equal iff (if and only if) they contain the same elements.

Thus if A, B are two equal sets,
then $A=B \Leftrightarrow \{x \in A \Leftrightarrow x \in B\}$.

For Ex. (I) If $A=\{2, 4, 6, 8\}$, $B=\{4, 6, 8, 2\}$, then $A=B$.
(II) If $C=\{-1, 1\}$, $D=\{x \mid x^2=1\}$, then $C=D$.

8. (*a*) **Sub-set and Super-set.**

If A and B are two sets such that every element of A is also an element of B, then

(*i*) *A is called a* **sub-set** *of B and*

(*ii*) *B is called a* **super-set** *of A.*

Symbolically (I) $A \subseteq B$ implies '*A is a sub-set of B*', i.e. '*A is included in B*'.
(II) $B \supseteq A$ implies '*B is a super-set of A*', i.e. '*B includes in A*'.

(*b*) **Proper and Improper Sub-sets.**

(*i*) *If A and B are two sets such that $A \subseteq B$ and $A \neq B$, then A is said to be proper sub-set of B.*

Symbolically. $A \subset B$ implies '*A is a proper sub-set of B*'.

(*ii*) *If A and B are two sets such that $A \subseteq B$ and $A=B$, then A is said to be improper sub-set of B.*

For Ex. (I) Every set is an improper sub-set of itself.
(II) Null set is a proper sub-set of every set.

Symbolically: (I) $A \not\subset B$ means that '*A is not a proper sub-set of B*'
(II) $A \not\supset B$ means that '*A is not a super-set of B.*

9. Comparable and Non-Comparable Sets.

(*i*) *If A and B are two sets such that either $A \subset B$ or $B \subset A$ then A and B are said to be* **comparable sets.**

For Ex. If $A=\{1, 3, 5, 7, 9\}$ and $B=\{3, 5, 7\}$,
then A and B are comparable sets because $B \subset A$.

(*ii*) *If A and B are two sets such that neither $A \subset B$ nor $B \subset A$ then A and B are said to be* **non-comparable sets.**

For Ex. If $A=\{1, 3, 5, 7, 9\}$ and $B=\{2, 4, 6, 8\}$, then A and B are non-comparable sets because neither $A \subset B$ nor $B \subset A$.

10. Universel Set. *A universal set is a set of which all the sets under consideration are sub-sets.*

For Ex. If A$=\{x \mid x$ is a prime number less than 50$\}$,

B$=\{x \mid x$ is a multiple of 6 between 5 and 55$\}$

and C$=\{x \mid x$ is a factor of 60$\}$,

then the set of natural numbers from 1 to 60 is a universal set, *i.e.*, X$=\{1, 2, 3, \ldots\ldots, 60\}$ is also a universal set.

Hence universal set is not unique.

11. Power Set. *The family of all sub-sets of a set S is called the power set of S.*

The power set of S is denoted by P(S).

For Ex. If A$=\{1, 2\}$,

then P(A)$=\{\phi, \{1\}, \{2\}, \{1, 2\}\}$.

Theorem. If a set contains n elements, then the number of its sub-sets is 2^n.

Proof. The number of sub-sets containing r elements

$=$The number of groups of r elements which can be formed out of n given elements, *i.e.*, ${}^nC_r$.

$\therefore$ No. of sub-sets containing no element $={}^nC_0$

No. of sub-sets containing 1 element $={}^nC_1$

No. of sub-sets containing 2 elements $={}^nC_2$

....

No. of sub-sets containing n elements $={}^nC_n$

$\therefore$ Total number of sub-sets$={}^nC_0+{}^nC_1+{}^nC_2+\ldots+{}^nC_n$

$=2^n$ [*Pre. U. Algebra*]

12. Disjoint Sets.

Two sets are said to be disjoint if they have not any element in common.

For Ex. The sets $\{1, 3, 5, 7, 9\}$ and $\{2, 4, 6, 8\}$ are disjoint because there is no common element.

OPERATIONS ON SETS

1. Union of Sets.

(*a*) **Union of two sets.** *Let A and B be two given sets. Then the union of the sets A and B is the set of all those elements which belong to A or to B or to both.*

The union of A and B is denoted by A$\cup$B and is read as *A union B*'.

Symbolically: A$\cup$B$=\{x \mid x\in$A *or* $x\in$B$\}$.

For Ex. If $A=\{1, 3, 5, 7\}$, $B=\{0, 1, 2, 3, 4\}$,
then $A \cup B=\{1, 3, 5, 7, 0, 2, 4\}$.

(*b*) **Union of more than two sets.** *Let $A_1, A_2, \ldots\ldots, A_n$ be n given sets. Then the union of these sets is the set of all the elements of these sets.*

The union of $A_1, A_2, \ldots\ldots\ldots, A_n$ is denoted by

$$A_1 \cup A_2 \cup \ldots\ldots\ldots \cup A_n \quad \text{or} \quad \bigcup_{i=1}^{n} A_i$$

Symbolically $\bigcup_{i=1}^{n} A_i=\{x \mid x \in A_i, \text{ for at least one } i\}$.

2. Intersection of Sets.

(*a*) **Intersection of two sets.** *Let A and B be two given sets. Then the intersection of the sets A and B is the set of all those elements which belong to both A and B.*

The intersection of A and B is denoted by $A \cap B$ and is read as '*A intersection B*'.

Symbolically $A \cap B=\{x \mid x \in A \text{ and } x \in B\}$.

For Ex. If $A=\{1, 3, 5, 7\}$, $B=\{0, 1, 2, 3, 4\}$,
then $A \cap B=\{1, 3\}$.

(*b*) **Intersection of more than two sets.** Let $A_1, A_2, \ldots, A_n$ be n given sets. Then the intersection of these sets is the set of all those elements each of which belongs to each of $A_1, A_2, \ldots\ldots, A_n$.

The intersection of $A_1, A_2, \ldots\ldots, A_n$ is denoted by

$$A_1 \cap A_2 \cap \ldots\ldots \cap A_n \quad \text{or} \quad \bigcap_{i=1}^{n} A_i$$

Symbolically $\bigcap_{i=1}^{n} A_i=\{x \mid x \in A_i \text{ for every } i\}$.

3. Difference of Sets.

If A and B are two sets, then their difference is the set of all those elements which belong to A and not to B.

The difference of sets A and B is denoted by $A-B$ and is read as '*A minus B*'.

Symbolically: $A-B=\{x \mid x \in A, x \notin B\}$.

For Ex. If $A=\{1, 2, 3, 4, 5, 6\}$ and $B=\{4, 5, 6, 7\}$,
then $A-B=\{1, 2, 3\}$.

☞ **Caution.** Generally $A-B \neq B-A$.

For Ex. If $A=\{1, 3, 5, 7, 9\}$ and $B=\{3, 5, 7, 9, 11\}$,
then $A-B=\{1\}$ and $B-A=\{11\}$.
Thus $A-B \neq B-A$.

4. Compliment of a Set.

The complement of a set A is the set of all those elements of the universal set X which do not belong to A.

The compliment of A is denoted by A^c.

Symbolically : $A^c = X - A = \{x \mid x \in X \text{ and } x \notin A\}$.

Another Def. A^c is the compliment of A in X
if $A \cup A^c = X$ and $A \cap A^c = \phi$.

For Ex. If $X=\{a, b, c, \ldots\ldots, x, y, z\}$ and $A=\{a, b, c\}$,
then $A^c=\{d, e, f, \ldots\ldots, x, y, z\}$.

(*i*) $A \cup A^c = \{a, b, c\} \cup \{d, e, f, \ldots\ldots, x, y, z\}$
$= \{a, b, c, \ldots\ldots, x, y, z\} = X$.

(*ii*) $A \cap A^c = \{a, b, c\} \cap \{d, e, f, \ldots\ldots, x, y, z\}$
$= \phi$.

ALGEBRA OF SETS

1. Properties of Union Operation.

Property I. *If A and B are any two sets, then*
(*i*) $A \subseteq (A \cup B)$ (*ii*) $B \subseteq (A \cup B)$.

Proof. (*i*) Let x be any member of the set A.
Then $x \in A \Rightarrow x \in A$ or $x \in B$
$\Rightarrow x \in (A \cup B)$.

Thus every member of A is also a member of $A \cup B$.
Hence $A \subseteq (A \cup B)$.

(*ii*) Please try yourself.

Property II. *If A is any set, then*
(*i*) $A \cup \phi = A$ (*ii*) $A \cup A = A$.
(*iii*) $A \cup X = X$, *where X is the universal set.*

Proof. In order to prove $A \cup \phi = A$, we have prove that
$A \subseteq (A \cup \phi)$ and $(A \cup \phi) \subseteq A$.

Clearly $A \subseteq (A \cup \phi)$ ...(1) [*By Property I*]

Now let x be any member of $A \cup \phi$.
Then $x \in A \cup \phi \Rightarrow x \in A$ or $x \in \phi$
$\Rightarrow x \in A$ [$\because$ *ϕ is an empty set*]

Thus $A \cup \phi \subseteq A$ ...(2)

Combining (1) and (2), $A \cup \phi = A$.

(*ii*) Please try yourself.

(*iii*) In order to prove $A \cup X = X$, we have to prove that

$$(A \cup X) \subseteq X \quad \text{and} \quad X \subseteq (A \cup X).$$

Clearly $A \cup X \subseteq X$ ...(1)

[$\because$ *Every set is a sub-set of the universal set*]

Also $X \subseteq A \cup X$ [*By Property I*] ...(2)

Combining (1) and (2), $A \cup X = X$.

Property III. Union of sets is commutative.

i.e. If A and B are any two sets, then $A \cup B = B \cup A$.

Proof. $x \in (A \cup B) \Leftrightarrow x \in A$ or $x \in B$

$\Leftrightarrow x \in B$ or $x \in A$

$\Leftrightarrow x \in (B \cup A)$

Hence $A \cup B = B \cup A$.

Property IV. Union of sets is associative.

i.e. If A, B and C are any three sets, then $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof. Suppose $P = (A \cup B) \cup C$ and $Q = A \cup (B \cup C)$.

To prove $P = Q$, we shall prove that $P \subseteq Q$ and $Q \subseteq P$

$x \in P \Leftrightarrow x \in (A \cup B)$ or $x \in C$

$\Leftrightarrow (x \in A$ or $x \in B)$ or $x \in C$

$\Leftrightarrow x \in A$ or $x \in B$ or $x \in C$

$\Leftrightarrow x \in A$ or $(x \in B$ or $x \in C)$

$\Leftrightarrow x \in A$ or $x \in (B \cup C)$

$\Leftrightarrow x \in Q$

Thus $P \subseteq Q$ ...(1)

and $Q \subseteq P$ ...(2)

Combining (1) and (2), $P = Q$.

2. Properties of Intersection Operation.

Property I. *If A and B are any two sets, then*

(*i*) $A \cap B \subseteq A$ (*ii*) $A \cap B \subseteq B$.

Proof. (*i*) Let x be any member of the set $A \cap B$.

Then $x \in (A \cap B) \Rightarrow x \in A$ and $x \in B$

$\Rightarrow x \in A$.

Hence $A \cap B \subseteq A$.

(*ii*) Please try yourself.

Property II. *If A is any set, then*

(*i*) $A \cap \phi = \phi$ (*ii*) $A \cap A = A$

(*iii*) $A \cap X = A$, *where X is the universal set.*

Proof. (*i*) In order to prove $A \cap \phi = \phi$, we have to prove that

$$\phi \subseteq (A \cap \phi) \quad \text{and} \quad (A \cap \phi) \subseteq \phi.$$

Clearly $A \cap \phi \subseteq \phi$ [*By Property I*] ...(1)

Since ϕ is the subset of every set,

$\therefore$ $\phi \subseteq A \cap \phi$ ...(2)

Combining (1) and (2), $A \cap \phi = \phi$.

(*ii*) Please try yourself.

(*iii*) In order to prove $A \cap X = A$, we have to prove that

$$A \cap X \subseteq A \quad \text{and} \quad A \subseteq A \cap X.$$

Clearly $A \cap X \subseteq A$ [*By Property I*] ...(1)

Let x be any member of A.

Then $x \in A \Rightarrow x \in X$

[$\because$ *Universal set is a super-set of every set*]

$\Rightarrow x \in A$ and $x \in X$

$\Rightarrow x \in A \cap X$.

Thus $A \subseteq A \cap X$ ...(2)

Combining (1) and (2), $A \cap X = A$.

Property III. Intersection of sets in commutative. *i.e. If A and B are any two sets, then* $A \cap B = B \cap A$.

Proof. $x \in (A \cap B) \Leftrightarrow x \in A$ and $x \in B$

$\Leftrightarrow x \in B$ and $x \in A$

$\Leftrightarrow x \in (B \cap A)$

Hence $A \cap B = B \cap A$.

Property IV. Intersection of sets is associative.

i.e., If A, B and C are any three sets, then

$$(A \cap B) \cap C = A \cap (B \cap C).$$

Proof. Suppose $P = (A \cap B) \cap C$ and $Q = A \cap (B \cap C)$.

To prove $P = Q$, we shall prove that $P \subseteq Q$ and $Q \subseteq P$.

$x \in P \Leftrightarrow x \in (A \cap B)$ and $x \in C$

$\Leftrightarrow (x \in A$ and $x \in B)$ and $x \in C$

$\Leftrightarrow x \in A$ and $x \in B$ and $x \in C$

$\Leftrightarrow x \in A$ and $(x \in B$ and $x \in C)$

$\Leftrightarrow x \in A$ and $x \in (B \cap C)$

$\Leftrightarrow x \in Q$.

Thus $P \subseteq Q$ ...(1)

and $Q \subseteq P$ ...(2)

Combining (1) and (2), $P = Q$.

3. Distributive Laws.

Law I. Intersection of sets is distributive over the union of sets.

i.e. If A, B, C are any three sets, then

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C).$$

Proof. In order to prove

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C),$$

we have to prove that

$$A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$$

and $$(A\cap B)\cup(A\cap C)\subseteq A\cap(B\cup C).$$

Let x be any member of $A\cap(B\cup C)$.

Then $x\in A\cap(B\cup C)\Leftrightarrow x\in A$ and $x\in(B\cup C)$

$\Leftrightarrow x\in A$ and ($x\in B$ or $x\in C$)

$\Leftrightarrow$($x\in A$ and $x\in B$) or ($x\in A$ and $x\in C$)

$\Leftrightarrow x\in(A\cap B)$ or $x\in(A\cap C)$

$\Leftrightarrow x\in(A\cap B)\cup(A\cap C)$

Thus $A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$

and $(A\cap B)\cup(A\cap C)\subseteq A\cap(B\cup C)$.

Hence $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

Law II. Union of sets is distributive over the intersection of sets.

i.e. If A, B, C are any three sets, then

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C).$$

Proof. Please try yourself.

4. Properties of Difference of Sets.

Property I. $A-B\neq B-A$ *i.e., difference of sets is not commutative.*

For Ex. If $A=\{1, 2, 3\}$ and $B=\{3, 4, 5\}$.

Then $A-B=\{1, 2\}$ and $B-A=\{4, 5\}$.

Thus $A-B\neq B-A$.

Hence the "difference of sets" is not commutative.

Property II. $(A-B)-C\neq A-(B-C)$

i.e., difference of sets is not associative.

For Ex. If $A=\{1, 2, 3\}$, $B=\{3, 4, 5\}$ and $C=\{1, 5, 6\}$,

then $(A-B)-C=\{1, 2\}-\{1, 5, 6\}=\{2\}$

and $A-(B-C)=\{1, 2, 3\}-\{3, 4\}=\{1, 2\}$

Thus $(A-B)-C=A-(B-C)$.

Hence the "*difference of sets*" is not associative.

Property III. *Prove that*

(*i*) $A \cup A^c = X$, *where X is the universal set*

(*ii*) $A \cap A^c = \phi$.

Proof. (*i*) In order to prove $A \cup A^c = X$, we have to prove that

$$A \cup A^c \subseteq X \quad \text{and} \quad X \subseteq A \cup A^c$$

Now $A \cup A^c \subseteq X$ ...(1)

[$\because$ *Every set is a subset of universal set*].

Also
$$\begin{aligned} x \in (A \cup A^c) &\Rightarrow x \in A \ \text{ or } \ x \in A^c \\ &\Rightarrow x \in A \ \text{ or } \ x \in (X - A) \\ &\Rightarrow x \in A \ \text{ or } \ (x \in X, x \notin A) \\ &\Rightarrow x \in X \end{aligned}$$

Thus $A \cup A^c \subseteq X$ ...(2)

Combining (1) and (2), $A \cup A^c = X$.

(*ii*) Please try yourself.

Property IV. *Prove that*

(*i*) $X^c = \phi$ (*ii*) $\phi^c = X$.

Proof. (*i*) In order to prove $X^c = \phi$, we have to prove that

$$X^c \subseteq \phi \quad \text{and} \quad \phi \subseteq X^c.$$

Now
$$\begin{aligned} x \in X^c &\Rightarrow x \notin X \\ &\Rightarrow x \in \phi \end{aligned}$$

[$\because$ *Every element belongs to X*]

Thus $X^c \subseteq \phi$ ...(1)

Also $\phi \subseteq X^c$ ...(2)

[$\because$ *Null set is a sub-set of every set*].

Combining (1) and (2), $X^c = \phi$.

(*ii*) Please try yourself.

Property V. *Prove that* $(A^c)^c = A$.

Proof.
$$\begin{aligned} (A^c)^c &= \{x \mid x \notin A^c\} \\ &= \{x \mid x \in A\} \\ &= A. \end{aligned}$$

5. De-Morgan's Laws.

(*i*) $(A \cup B)^c = A^c \cap B^c$

(*ii*) $(A \cap B)^c = A^c \cup B^c$.

Proof. Let X be the universal set so that every x under consideration $\in X$.

(*i*) $(A \cup B)^c = \{x \mid x \notin (A \cup B)\}$
$= \{x \mid x \notin A \text{ and } x \notin B\}$
$= \{x \mid x \in A^c \text{ and } x \in B^c\}$
$= A^c \cap B^c$.

(*ii*) Please try yourself.

Definitions :

1. Ordered Pairs. *An ordered pair contains two elements; say a, b so that a is given the first place and b the second place.*

This is denoted by (a, b).

2. Cartesian Product of two Sets.

Let A and B be any two sets, then the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$ is called the cartesian product of A and B.

This is denoted as $A \times B$ and is read as '*A cross B*'.

Symbolically $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

For Ex. If $A = \{1, 2, 3\}$ and $B = \{a, b\}$,

then $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$

and $B \times A = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.

Thus $A \times B \neq B \times A$.

Hence commutative law does not hold.

3. Cartesian Product of three Sets.

Let A, B and C be any three sets, then the set of all ordered triples (a, b, c), where $a \in A$, $b \in B$ and $c \in C$ is called the cartesian product of A, B and C.

This is denoted as $A \times B \times C$ and is read as '*A cross B cross C*'

Symbolically $A \times B \times C = \{(a, b, c) \mid a \in A, b \in B, c \in C\}$.

For Ex. If $A = \{1, 2\}$, $B \{4, 5\}$, $C = \{6, 7\}$,

then $A \times B \times C = \{(1, 4, 6), (1, 4, 7), (1, 5, 6), (1, 5, 7), (2, 4, 6), (2, 4, 7), (2, 5, 6), (2, 5, 7)\}$

4. Cartesian Product of Sets.

Let $A_1, A_2, \ldots, A_n$ be any n sets, then the set of all ordered n triples $(a_1, a_2, \ldots, a_n)$, where $a_1 \in A_1$, $a_2 \in A_2$, ..., $a_n \in A_n$ is called the cartesian product of $A_1, A_2, \ldots, A_n$.

This is denoted as $A_1 \times A_2 \times \ldots \times A_n$ and is read as
'*A_1 cross A_2 cross...... cross A_n*'.

Symbolically: $A_1 \times A_2 \times \ldots \times A_n$
$= \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$.

SECTION—B

MAPPINGS OR FUNCTIONS

(a) Definitions :

1. **Mapping.** *Let A and B be two non-empty sets. Then a* **mapping** (*or a* **function**) *from a set A to a set B is a rule which associates to each element of A, a unique element of B.*

This is also known as **transformation** *or* **operator.**

This is denoted by $f: A \to B$ or $A \xrightarrow{f} B$,
and is read as '*f is a function of A to B*'.

2. **f-image and pre-image.**

Let $f: A \to B$. Further let $x \in A$, $y \in B$ such that $f(x)=y$, then y is called the **f-image** *of x, and is usually denoted by $f(x)$.*

Here x is called the **pre-image** *of y.*

3. **Domain and Co-domain.**

Let $f: A \to B$. Further let $x \in A$, $y \in B$ such that $f(x)=y$, then the set A is called the **domain** *of f and the set B is called the* **co-domain** *of f.*

4. **Range.**

Let $f: A \to B$, then the set of the images of all elements of A is called the range of f.

The range of f is denoted by $f(A)$.

Symbolically i $f(A)=\{f(x) \mid x \in A\}$.

(b) Types of Mappings.

1. **Into Mapping.** *Let $f: A \to B$ such that there is at least one element B which is not the f-image of some element of A, then f is said to be mapping of A* **into** *B.*

Symbolically : $f: A \to B$ is **into**

iff $\{f(x)\} \subset B$, where $x \in A$ and $\{f(x)\}=$ Range set of f.

2. **Onto Mapping :** *Let $f: A \to B$ such that each element of B is f-image of at least one element of A, then f is said to be mapping of A* **onto** *B.*

Symbolically : $f: A \to B$ **is into**

iff $\{f(x)\}=B$, where $x \in A$ and $\{f(x)\}=$ Range set of f.

Onto mapping is also called **subjection** or **surjective mapping**.

3. **One-one Mapping.** *Let $f: A \to B$ such that different elements in A have different images in B, then f is said to be one-one mapping.*

Symbolically : $f: A \to B$ is **one-one** if $x_1, x_2 \in A$,

$$f(x_1)=f(x_2) \Rightarrow x_1=x_2$$

or

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

One-one mapping is also called **injection** or **injective mapping.**

One-one and onto mapping is called **bijection** or **bijective mapping.**

4. Many-one Mapping. *Let $f: A \to B$ such that two or more different elements in A have the same image in B, then f is said to be many-one mapping.*

Symbolically : $f: A \to B$ is **many-one** if $x_1, x_2 \in A$,

$$f(x_1)=f(x_2) \Rightarrow x_1 \neq x_2.$$

Conclusion :

If $f: A \to B$, then f is (*i*) one-one into mapping or (*ii*) one-one onto mapping or (*iii*) many-one into mapping or (*iv*) many-one onto mapping.

5. Identity Mapping. *Let $f: A \to A$, then f is said to be an identity mapping if each element is mapped on itself.*

This is denoted by I.

Symbolically : Let $f: A \to A$. Then f is identity mapping if $f(x)=x \ \forall \ x \in A$.

Remember : **Identity mapping is one-one onto.**

Example 1. *Let $A=\{1, 2, 3\}$ and $B=\{4, 5\}$. Classify the following* :

(*i*) $f_1=\{(1, 4), (2, 5), (3, 5)\}$

(*ii*) $f_2=\{(1, 4), (2, 5)\}$.

Sol. (*i*) The mapping is many-one onto.

(*ii*) The mapping is not defined because there is no image of 3.

Example 2. *Let f : $\mathbf{R} \to \mathbf{R}$, classify the following* :

(*i*) $f(x)=2x$ *where* $x \in \mathbf{R}$

(*ii*) $f(x)=x^2$ *where* $x \in \mathbf{R}$.

Sol. (*i*) This mapping is one-one onto.

(*ii*) This mapping is many-one into.

Example 3. *Let f : $\mathbf{R} \to \mathbf{R}$, classify the following* :

(*i*) $f(x)=x^2$ (*ii*) $f(x)=e^x$

(*iii*) $f(x)=\log x$ (*iv*) $f(x)=\tan x$.

Sol. (*i*) The mapping is one-one

because $f(x_1)=f(x_2) \Rightarrow x_1^2=x_2^2 \Rightarrow x_1=x_2$.

Again since every real number a has a square root,

$\therefore \quad f(\sqrt{a})=(\sqrt{a})^2=a.$

This shows that the image of f is whole set of real numbers, and thus the mapping is onto.

Hence f is **one-one onto.**

(*ii*) The mapping is one-one

because $f(x_1)=f(x_2) \Rightarrow e^{x_1}=e^{x_2} \Rightarrow x_1=x_2$.

Again let x be any positive element of **R**.

Then $f(x)=e^x$ *i.e.* +ve real number

and $f(-x)=e^{-x}=\dfrac{1}{e^x}$ *i.e.* +ve real number.

Thus since no real number is mapped on any negative real number and therefore the mapping is into.

Hence f is **one-one into.**

(*iii*) Here f is not defined

because log (−ve real number) is not defined.

(*iv*) The mapping is many-one because there exists many angles whose tangent is the same real number.

[$\because$ $\tan(2n\pi+\theta)=\tan\theta$]

Again the mapping is onto because corresponding to each real number y there exists a real number x such that $x=\tan^{-1} y$.

Hence f is **many-one onto.**

Example 4. *Prove that the function* $f: \mathbf{R}\to\mathbf{R}$ *defined by* $f(x)=\cos x$ *is neither one-one nor onto.*

Sol. Let $x_1, x_2 \in \mathbf{R}$.

Then $f(x_1)=f(x_2) \Rightarrow \cos x_1=\cos x_2$,

which does not imply that $x_1=x_2$.

Thus f is not one-one.

Again since $\cos x$ lies between -1 and 1 only,

$\therefore$ there exist many real numbers which are not the images of any real number.

Thus f is not into.

Hence f is neither one-one nor onto.

More Definitions :

1. Constant Mapping. *Let* $f: A\to B$. *Then* f *is said to be constant mapping if every element of* A *is mapped on the same element of* B.

Range of f has only one element.

2. Equality of Mappings. *Let $f: A \to B$ and $g: A \to B$. Then the mappings are said to be equal if $f=g \ \forall \ x \in A$.*

3. Inverse Mapping. *Let $f: A \to B$ be one-one onto mapping. Then $f^{-1}: B \to A$, where $f(a)=b$, i.e., $b \in B$ is the image of $a \in A$ under f, is called the inverse mapping of f.*

Theorem I. *If $f: A \to B$ is one-one into, then $f^{-1}: B \to A$ is also one-one onto.*

Proof. Let x_1, x_2 be any two different elements of A whose images are y_1, y_2 such that $f(x_1)=y_1$ and $f(x_2)=y_2$ ...(1)

If f^{-1} is the inverse of f, then

$$f^{-1}(y_1)=x_1 \text{ and } f^{-1}(y_2)=x_2 \quad \text{...(2)}$$

Since f is one-one,

$\therefore \quad x_1 \neq x_2 \quad \Leftrightarrow \quad f(x_1) \neq f(x_2)$

i.e. $f^{-1}(y_1) \neq f^{-1}(y_2) \Leftrightarrow \quad y_1 \neq y_2$ [*From (1) and (2)*]

Thus f^{-1} is one-one ...(3)

Since f is onto, [*Given*]

$\therefore$ all different elements of B are f-images of different elements of A.

$\Rightarrow$ all different elements of A are f^{-1} images of different elements of B

$\Rightarrow$ f^{-1} is onto ...(4)

Combining (3) and (4), f^{-1} is one-one onto.

Theorem II. *If $f: A \to B$ is one-one onto, then prove that $f^{-1}: B \to A$ is unique.*

Proof. Let $g: B \to A$ and $h: B \to A$ be two universe mappings of $f: A \to B$.

To prove : f^{-1} is unique, *i.e.*, $g=h$.

Let y be an element of B.

Let $g(y)=x_1 \Rightarrow f(x_1)=y$.

Again since h is the inverse mapping of f,

$\therefore \quad h(y)=x_2 \Rightarrow f(x_2)=y$.

Since f is one-one, [*Given*]

$\therefore \ f(x_1)=f(x_2) \Rightarrow x_1=x_2$ [*Def.*]

$\Rightarrow g(y)=h(y)$

$\Rightarrow g=h$.

Hence f^{-1} is unique.

4. Composite mapping (Product of Mappings).

Let $f: A \to B$ and $g: B \to C$ be two mappings such that $f(x)=y$ and $g(y)=z$, where $x \in A$, $y \in B$, $z \in C$.
Then the mapping $h: A \to C$ such that
$$h(x)=z=g(y)=g\{f(x)\} \ \forall \ x \in A$$
is called the composite mapping (or product of mappings) of f and g.

The above composite mapping is usually denoted by $g \circ f$ and is read as '*g operation f*'.

Caution. In $(g \circ f)$, we operate first by f and then by g.

The composite of mappings is not commutative.

For Ex. If $f(x)=x^3$ and $g(y)=y^2+1$,
then $(g \circ f)(x)=g[f(x)]=g(x^3)=x^6+1$
and $(f \circ g)(x)=f[g(x)]=f(x^2+1)=(x^2+1)^3$.
Thus $f \circ g \neq g \circ f$.
Hence product of mappings is not commutative.

Theorem III. Associativity of mappings.

Let $f: A \to B$, $g: B \to C$, $h: C \to D$.
Then $(h \circ g) \circ f = h \circ (g \circ f)$.

Proof. Let x be any member of A.
$$\begin{aligned}[(h \circ g) \circ f](x) &= (h \circ g)[f(x)] \\ &= h[g[f(x)]] \\ &= h[(g \circ f)x] \\ &= [h \circ (g \circ f)]x.\end{aligned}$$
Hence $(h \circ g) \circ f = h \circ (g \circ f)$.

Theorem IV. The product of any function with the identity function is the function itself.

i.e. if $f: A \to B$, then $f \circ I_A = f = I_B \circ f$.

Proof. Let x be any member of A.
Then $f(x)=y$, where $x \in$ A and $y \in$ B ...(1)
Now $f: A \to B$ and $I_B: B \to B$, then $I_B \circ f: A \to B$.
Also $(I_B \circ f)(x)=I_B(f(x))=I_B(y)$ [*From (1)*]
$=y$ [$\because$ *I_B is the identity mapping on B*]
$=f(x)$
Thus $I_B \circ f=f$ ...(A)
Again $\because$ $I_A: A \to A$ and $g: A \to B$
$\therefore$ $f \circ I_A: A \to B$
$\therefore$ $(f \circ I_A)(x)=f(I_A(x))=f(x)$ ...(B)
[$\because$ *I_A is the identity mapping on A*]
Combining (A) and (B), we have
$$f \circ I_A = f = I_B \circ f.$$

SECTION—C
RELATIONS

(*a*) **Def.** *If A and B are two sets, then a relation from A to B is the subset of* $A \times B$.

Let $x \in A$ and $y \in B$.

(*i*) '*x is related to y*' is written as xRy.

(*ii*) '*x is not related to y*' is written as $x \not R y$.

For Ex. Let A=set of teachers in the college,
B=set of students in the college.

Further let $x \in A$ and $y \in B$,

then xRy if x is a teacher of y.

Here R, the relation is '*is a teacher of*'.

Symbolically : $R = \{(x, y) \mid x \in A, y \in B, x \text{ is a teacher of } y\}$.

(*b*) **Types of Relations.**

(*i*) **Reflexive Relation.** *A relation R in a set A is said to be reflexive if* $(a, a) \in R \ \forall \ a \in A$

i.e., if $aRa \quad \forall a \in A$.

For Ex. The relation '*is parallel to*' in the set of all st. lines in a plane is reflexive **because** every st. line in a plane is parallel to itself.

(*ii*) **Symmetric Relation.** *A relation R in a set A is said to be symmetric if* $(a, b) \in R \Rightarrow (b, a) \in R$

i.e., if $aRb \Rightarrow bRa$.

For Ex. The relation '*is the brother of*' in the set of all men is symmetric beeause if a, b are two men,

then a is a brother of $b \Rightarrow b$ is a brother of a.

(*iii*) **Transitive Relation.** A relation R in a set A is said to be transitive if $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$

i.e. if aRb and $bRc \Rightarrow aRc$.

For Ex. The relation '*is the sister of*' in the set of all human beings is transitive **because** if a is the sister of b, b is the sister of c, then a is the sister of c.

(*iv*) **Equivalence Relation.** *A relation R in a set A is said to be an equivalence relation if it is*

(I) *reflexive* (II) *symmetric and* (III) *transitive.*

For Ex. *The relation R ('is congruent to') in the set A (set of all triangles in a plane) is an equivalence relation.*

R is an equivalence relation **because**

(I) R is reflexive

[$\because$ $aRa \ \forall a \in A$ since each triangle is congruent to itself.]

(II) R is symmetric [$\because$ $a\text{R}b \Rightarrow b\text{R}a$ since $a \equiv b \Rightarrow b \equiv a$]

(III) R is transitive

[$\because$ $a\text{R}b, b\text{R}c \Rightarrow a\text{R}c$ since $a \equiv b, b \equiv c \Rightarrow a \equiv c$]

SECTION—D

THEORY OF NUMBERS

1. Definitions.

(*i*) The numbers.........$-4, -3, -2, -1, 0, 1, 2, 3, 4,$ .... are called **integers.**

(*ii*) The numbers......0,1, 2, 3, 4,......are called **non-negative integers.**

(*iii*) The numbers ....1, 2, 3, 4,.........are called **positive integers** or **natural numbers** or **whole numbers** or **counting numbers.**

2. Peano Axioms.

Peano, an Italian Mathematician, gave us the following axioms of the set **N** of natural numbers in 1899 A.D.

Axiom I. $1 \in \mathbf{N}$ *i.e. 1 is a natural number.*

Conclusion : $\mathbf{N} \neq \phi$.

Axiom II. *For every $n \in N$, there exists a unique natural number $n^+ (= n+1)$.*

Remember : n^+ is called the successor of n.

Conclusion. Set of natural numbers is infinite.

Axiom III. *For no $n \in N$, $n^+ = 1$ i.e. 1 is not the successor of any natural number.*

Conclusion. 1 is the least natural number.

3. Divisibility.

(*a*) **Def.** *An integer $a (\neq 0)$ is said to divide another integer b if there exists another integer c such that $b = ca$.*

Here b is a **multiple** of a.

Symbolically. We write a/b

In case b is not divisible by a, we write $a \nmid b$.

Cautions : (I) Never take 0 for a in a/b

(II) $a/0$ holds good provided $a \neq 0$.

For Ex. (I) $2 \mid 6$ since $6 = 3.2$

(II) $3 \nmid 7$ since 7 is not divisible by 3

(III) $a/0$ since $0 = a.0$ where $a \neq 0$

(IV) $1/a$ for any integer a

(V) a/a for any integer a.

Note. If a/b, then $a/-b$, $-a/b$, $-a/-b$.

THEOREMS

Theorem I. *If a/b and b/c, then a/c.*

Proof. Since a/b,

$\therefore$ there exists an integer m s.t. $b=m \cdot a$ ...(1)

Again since b/c,

$\therefore$ there exists an integer n s.t. $c=n \cdot b$ ...(2)

Putting the value of b from (1) in (2), we get

$$c=n(ma)=(nm)a$$

Hence by def., a/c. [$\because$ *nm is an integer*]

Theorem II. *If ac/bc, then a/b.*

Proof. Since $ac \neq 0$, $\therefore$ both $a \neq 0$ and $c \neq 0$

As ac/bc.

$\therefore$ there exists an integer m s.t.

$$bc=(ac)m \quad i.e. \quad bc=m(ac)$$

$$\Rightarrow \quad b=ma \quad \Rightarrow \quad a/m.$$

Theorem III. *If a/b and $c \neq 0$, then ac/bc.*

Proof. Since a/b,

$\therefore$ there exists an integer m s.t. $b=ma$.

Multiplying both sides by c, we have.

$$bc=(ma)c$$

$$\Rightarrow \quad bc=m(ac)$$

$$\Rightarrow \quad ac/bc.$$

Theorem IV. *If a/b, then a/bx for any integer x.*

Proof. Since a/b,

$\therefore$ there exists an integer m s.t. $b=ma$.

Multiplying both sides by x, we have

$$bx=(ma)x \quad \Rightarrow \quad bx=(mx)a$$

$\Rightarrow$ a/bx [$\because$ *mx is an integer*]

Theorem V. *If a/b and a/c, then $a/(b+c)$ and $a/(b-c)$.*

Proof. Since a/b,

$\therefore$ there exists an integer m s.t. $b=ma$ ...(1)

Since a/c,

$\therefore$ there exists an integer n s.t. $c=na$ ...(2)

(*i*) Adding (1) and (2),

$$b+c=(m+n)a \quad \Rightarrow \quad a/(b+c)$$

[$\because$ *$(m+n)$ is an integer*]

(*ii*) Subtracting (2) from (1),

$$b-c=(m-n)a \quad \Rightarrow \quad a/(b-c).$$

[$\because$ *$(m-n)$ is an integer*]

Theorem VI. *If a/b, a/c, then $a/(bx \pm cy)$, where x, y are any integers.*

Proof Since a/b,

$\therefore$ as above $b = ma$

Multiplying by x, $bx = (ma)\,x$ ...(1)

Since a/c, $\therefore$ as above, $c = na$

Multiplying by y, $cy = (na)y$ ...(2)

(*i*) Adding (1) and (2),

$$bx + cy = a(mx + ny)$$

$\Rightarrow$ $a/(bx + cy)$

[$\because$ *$mx + ny$ is an integer as m, n, x, y are all integers*]

(*ii*) Subtracting (2) from (1),

$$bx - cy = a(mx - ny)$$

$\Rightarrow$ $a/(bx - cy)$ [$\because$ *$mx - ny$ is an integer*]

Theorem VII. *If a/b and $b < a$, where a, b are non-integers and $c \neq 0$, then $b = 0$.*

Proof. Since a/b,

$\therefore$ there exists an integer m s.t. $b = ma$

$\Rightarrow$ $b \geqslant a$ ...(1)

But $b < a$ ...(2) [*Given*]

(1) and (2) lead to contradiction.

The theorem is true only when $b = o$.

[$\because$ *Every non-zero integer divides 0*]

4. Classification.

Natural numbers are divided into three classes :

(*i*) Unit (*ii*) Prime (*iii*) Composite.

(*i*) **Unit.** *1 is the only unit in natural numbers.*

(*ii*) **Prime.** *A natural number $a(>1)$ is said to be prime if it is divisible only by 1 and a itself.*

For Ex. 2, 3, 5, 7, 11,...... are all prime numbers.

(*iii*) **Composite.** *A natural numbers a (>1) is said to be composite if it has least one more divisor except 1 and itself.*

For Ex. 4, 8, 12, ... are all composite numbers.

Remember. 1 is neither prime nor composite. Prime number has two divisors.

Composite number has at least three divisors.

Remark : In the set of integers,

Units are ± 1.

Prime. An integer a is said to be prime if it is divisible by ± 1, $\pm a$.

5. Algorithm

(*i*) **Def.** *Any mathematical process, in which every step depends upon the preceding step is called algorithm.*

(*ii*) **Division Algorithm.** The process of simple division is known as division algorithm.

Theorem. *Given any two integers a and b, there exists unique integers q and r such that*

$$a = bq + r, \text{ where } 0 \leq r < b.$$

Here q is called the **quotient** and r the **remainder.**

6. Greatest Common Divisor

(*i*) **Common Divisor. Def.** If c/a *and* c/b, *then c is called common divisor of a and b.*

(*ii*) **Greatest Common Divisor. Def.** *If a number d divides both a and b and is the greatest of all the common divisors of a and b, then d is called the greatest common divisor* (*g.c.d.*) *of a and b.*

In other words. *d is said to be the g.c.d. of a and b if*

(*i*) d/a *and* d/b

(*ii*) c/d, *where c is any other common divisor of a and b.*

Notations. *g.c.d.* of a and b is denoted by (a, b).

g.c.d. of $a, b, c, \ldots\ldots$ is denoted by $(a, b, c, \ldots\ldots)$.

For Ex. $(4, 6) = 2$ because *g.c.d.* of 4 and 6 is 2.

Remember. $\boxed{(a, b) = (b, a)}$

Remark. If $b \mid a$, *then* $(a, b) = b$.

(*iii*) **Relatively Prime Integers** (or **Coprime Integers**).

Def. *Two integers a and b whose greatest common divisor* $d = (a, b) = 1$ *are said to be relatively prime or coprime.*

Remember : $\boxed{(a, b) = 1 \Leftrightarrow a, b \text{ are coprime}}$

For Ex. 4 and 7 are coprime integers because $(4, 7) = 1$.

Caution. Two integers which are coprime, may not be prime integers.,

7. Least Common Multiple.

(*i*) **Common Multiple. Def.** *If* a/m *and* b/m, *then m is called common multiple of a and b.*

(*ii*) **Least Common Multiple. Def.** *If a number n is divided by both a and b and is the least of all the common multiples of a and b, then n is called the least common multiple* (*l. c. m.*) *of a and b.*

Notations. *l.c.m.* of a and b is denoted by $[a, b]$
l.c.m. of $a, b, c, \ldots\ldots$ is denoted by $[a, b, c, \ldots\ldots]$

For Ex. $[4, 6]=12$.

Remark. *If p is prime, then either p/a or $(p, a)=1$.*

Proof. Let $(p, a)=d$

$\therefore$ d/p and d/a [*Def.*]

Now d/p and p is a prime number

$\therefore$ either $d=1$ or $d=p$

[$\because$ *Divisors of prime number p are 1 and p*]

When $d=1$, then $(p, a)=1$.

When $d=p$, then $(p, a)=p \Rightarrow p/a$.

Theorem I. *If $a=bq+r$, then $(a, b)=(b, r)$.*

Theorem II. *If $d=(a, b)$, there exist integers x and y such that $d=ax+by$.*

Cor. If a, b are relatively prime, then $1=ax+by$.

Theorem III. *If a/bc and $(a, b)=1$, then a/c.*

Proof. Since a/bc, [*Given*]

$\therefore$ there exists an integer d st. $bc=ad$ ...(1)

Again since $(a, b)=1$, [*Given*]

$\therefore$ by above Cor., there exist integers x and y s.t. $1=ax+by$

Multiplying by c,

$$c=acx+bcy$$
$$\Rightarrow \quad c=acx+ady \qquad [\textit{From (1)}]$$
$$\Rightarrow \quad c=a(cx+dy)$$
$$\Rightarrow \quad a/c.$$

Theorem IV. *If $(a, b)=d$, then $(a/d, b/d)=1$.*

Theorem V. *If p is prime and p/ab, then either p/a or p/b.*

Proof. Since p/ab,

$\therefore$ $ab=pd$, where d is an integer ...(1)

Let us suppose that $p \nmid a$

$\therefore$ p is co-prime to a [$\because$ *p is prime*]

$\therefore$ $px+ay=1$, where x, y are integers. ...(2)

Multiplying (2) by b,

$$bpx+bay=b$$
$$\Rightarrow \quad pbx+aby=b$$
$$\Rightarrow \quad pbx+pdy=b \qquad [\textit{From (1)}]$$
$$\Rightarrow \quad p(bx+dy)=b$$

Hence p/b [$\because$ *bx+dy is an integer*]

8. Definitions.

(*i*) *Let m be a +ve integer. Two integers a and b are said to be* **congruent modulo m** *if m divides $(a-b)$ and are expressed as $a \equiv b \pmod{m}$.*

This is so if $m/(a-b)$.

For. Ex. $15 \equiv 1 \pmod{14}$ because $14 \times 1 + 1 = 15$
$26 \equiv 1 \pmod 5$ because $5 \times 5 + 1 = 26$
$18 \equiv 0 \pmod 6$ because $6 \times 3 + 0 = 18$
$153 \equiv -7 \pmod 8$ because $8 \times 20 - 7 = 153$.

(*ii*) If $a \equiv b \pmod m$, then $m/a-b$

$$\Rightarrow (a-b) = mq$$
$$\Rightarrow \quad a = mq + b.$$

Theorem. *The relation congruence modulo m is an equivalence relation in the set of integers.*

Proof. [A relation is said to be an equivalence if it is reflexive, symmetric and transitive.]

(*i*) **Reflexive** : $a \equiv a \pmod m$

Since m/o *i.e.* $m/(a-a)$,

$\therefore \quad a \equiv a \pmod m$ [*Def.*]

Thus reflexive property is established.

(*ii*) **Symmetric.** $a \equiv b \pmod m \quad \Rightarrow b \equiv a \pmod m$

$a \equiv b \pmod m \Rightarrow m/(a-b) \quad \Rightarrow m/-(a-b)$

$\Rightarrow m/(b-a) \quad \Rightarrow b \equiv a \pmod m$ [*Def.*]

Thus symmetric property is established.

(*iii*) **Transitive.** $a \equiv b \pmod m$, $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

$a \equiv b \pmod m \quad \Rightarrow m/(a-b)$

$b \equiv c \pmod m \quad \Rightarrow m/(b-c)$

$\Rightarrow m/[(a-b)+(b-c)] \Rightarrow m/(a-c)$

$\Rightarrow a \equiv c \pmod m$ [*Def.*]

Thus transitive property is established.

From (*i*), (*ii*), (*iii*), the relation congruence modulo is an equivalence relation.

9. Residue Classes.

The relation "congruent modulo m" has m distinct equivalence classes, called residue classes or congruence classes modulo m.

For Ex. Residue classes of modulo 7 are

$\{0\} = \{\ldots\ldots -14, -7, 0, 7, 14, \ldots\ldots\}$
$\{1\} = \{\ldots\ldots -13, -6, 1, 8, 15, \ldots\ldots\}$
$\{2\} = \{\ldots\ldots -12, -5, 2, 9, 16, \ldots\ldots\}$
....
$\{6\} = \{\ldots\ldots -8, -1, 6, 13, 20 \ldots \ldots\}$.

Example. *Form the addition and multiplication table for the set of residue classes mod 6.*

Sol. For convenience we write 0, 1, 2, 3, 4, 5 in place of {0}, {1}, {2}, {3}, {4}, {5} respectively.

(*i*) **Addition Table**

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

because

$1+5=6\equiv 0 \pmod 6$

$2+4=6\equiv 0 \pmod 6$

$2+5=7\equiv 1 \pmod 6$

$3+5=8\equiv 2 \pmod 6$; etc.

(*ii*) **Multiplication Table**

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

because

$2\times 3=6\equiv 0 \pmod 6$

$2\times 5=10\equiv 4 \pmod 6$

$4\times 5=20\equiv 2 \pmod 6$; etc.

SECTION E
REAL NUMBER SYSTEM

1. Binary Composition.

When there exists a rule according to which every ordered pair of elements of the given set A gives a unique member of the set A, then this rule is known as binary composition or binary operation.

Briefly. A binary operation on a set A is mapping oı $A\times A$ into A.

This is generally denoted by o, $*$, $\cdot$; etc.

2. (*i*) Number System.

A set A is said to be a number system if two binary operations are defined on A such that

(I) *both the operations are commutative* ;

(II) *both the operations are associative*

and (III) *one operation is distributive over the other.*

(*ii*) **Number.** *Each element of the number system is said to be a number.*

Examples :

1. Natural Numbers. *Consider* (N, + , .).

Here N={1, 2, 3,......} is a set of natural numbers. This set possesses two binary operations : addition (+) and multiplication ($\cdot$).

Now (N, + , .) is a number system because

(I) both operations are commutative

(II) both operations are associative

Pan (III) multiplication is distributive over addition.

2. Integers. Consider (I, +, .)

Here $I = \{\ldots\ldots\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\ldots\}$ is a set of integers. This set possesses two binary operations: addition (+) and multiplication (.).

Now (I, +, .) is a number system because

(I) both operations are commutative

(II) both operations are associative

and (III) multiplication is distributive over addition.

3. Rational Numbers. Consider (Q, + .).

Here $Q = \left\{ \frac{p}{q} \middle/ p, q \in I, \quad q \neq 0, \quad q > 0 \right\}$ is a set of all rational numbers.

This set possesses two binary operations : addition (+) and multiplication ($\cdot$).

Now (Q, + .) is a number system because

(I) both operations are commutative

(II) both operations are associative

and (III) multiplication is distributive over addition.

2

Groups

DEFINITIONS

1. Group.

A system $<G, *>$, where G is non-empty set and $*$ is a binary composition on G, is called a group if it satisfies the following postulates : [G.N.D.U. 1981]

(*i*) **Closure Axiom** : $\forall\ a, b \in G \Rightarrow a * b \in G$.

(*ii*) **Associative Law** : $a*(b*c)=(a*b)*c\ \forall a, b, c \in G$.

(*iii*) **Existence of Identity** : *There exists an element* $e \in G$, *called an* **identity**, *such that* $a*e=a=e*a\ \forall a \in G$.

(*iv*) **Existence of Inverse** : $\forall a \in G$, *there exists an element* $a^{-1} \in G$, *called the* **inverse** *of a, such that* $a*a^{-1}=e=a^{-1}*a$.

Caution. a^{-1} does not mean $\frac{1}{a}$.

2. Commutative Group or Abelian Group.

If in addition to the above four postulates, the following postulate is also satisfied, the group G is called a Commutative or an Abelian group.

(*v*) **Commutative Law.** $\forall a, b \in G,\ a*b=b*a$.

3. Non-Commutative Group or Non-abelian Group.

If the group does not satisfy the above postulate (v), *then the group G is called Non-Commutative or Non-abelian group.*

4. Finite and Infinite Group.

If the number of elements in the group G is finite, then $<G, *>$ *is called a finite group, otherwise it is called an infinite group.*

5. Order of Group.

The number of elements in a finite group is called the order of the group.

This is denoted by O(G) or $|G|$.

The infinite group is of infinite order.

6. Semi-Group.

A system $<G, *>$, *where G is a non-empty set and* $*$ *is a binary composition on G, is called a semi-group if it satisfies the following postulates :*

(*i*) **Closure Axiom** : $\forall a, b \in G \Rightarrow a*b \in G$.

(*ii*) **Associative Law** : $a*(b*c)=(a*b)*c\ \forall a, b, c \in G$.

Conclusion : Every group is a semi-group but every semi-group may or may not be a group.

Example 1. *Prove that* $<Z, +>$, *where* Z *is a set of all integers, is an infinite abelian group.*

Sol. The system is $<Z, +>$, where

$Z=\{......-3, -2, -1, 0, 1, 2, 3,......\}$ and '+' is the binary composition in Z.

(*i*) **Closure Axiom.** $\forall\ a, b \in Z \Rightarrow a+b \in Z.$

[$\because$ *Sum of any two integers is an integer*]

(*ii*) **Associative Law** : $a+(b+c)=(a+b)+c\ \ \forall a, b, c \in Z.$

(*iii*) **Existence of Identity.** There exists an element $0 \in Z$, such that $a+0=a=0+a\ \ \forall a \in Z.$

(*iv*) **Existence of Inverse.** $\forall a \in Z$, there exists an element $-a \in Z$, such that $a+(-a)=0=(-a)+a.$

[**Remember** : $-a$ *is the inverse of* a *under addition.*]

Thus $<Z, +>$ *is a group.*

(*v*) **Commutative Law.** $\forall a, b \in Z,\ a+b=b+a.$

Thus $<Z, +>$ *is an abelian group.*

(*vi*) Since the number of integers is infinite,

$\therefore$ Z is an infinite set.

Hence $<Z, +>$ **is an infinite abelian group.**

Example 2. *Prove that* $<Q, +>$, *where Q is a set of rational numbers, is an infinite abelian group.*

Sol. The system is $<Q, +>$, where Q is a set of rational numbers and '+' is the binary operation in Q.

(*i*) **Closure Axiom.** $\forall a, b \in Q \Rightarrow a+b \in Q.$

[$\because$ *Sum of any two rational numbers is a rational number*]

(*ii*) **Associative Law.** $a+(b+c)=(a+b)+c\ \ \forall a, b, c \in Q.$

(*iii*) **Existence of Identity.** There exists an element $0 \in Q$ such that $a+0=a=0+a\ \ \forall a \in Q.$

(*iv*) **Existence of Inverse.** $\forall a \in Q$, there exists an element $-a \in Q$ such that $a+(-a)=0=(-a)+a.$

Thus $<Q, +>$ *is a group.*

(*v*) **Commutative Law.** $\forall a, b \in Q,\ a+b=b+a.$

Thus $<Q, +>$ *is an abelian group.*

(*vi*) Since the number of rational numbers is infinite,

$\therefore$ Q is an infinite set.

Hence $<Q, +>$ **is an infinite abelian group.**

Example 3. *Prove that* $<R, +>$, *where R is a set of real numbers is an infinite abelian group.*

Sol. Similar to Ex. 2. [Replace Q by R]

Example 4. *Prove that $<C, +>$, where **C** is a set of complex numbers is an infinite abelian group.*

Sol. The system is $<C, +>$, where C is a set of complex numbers and '+' is the binary operation in C.

(*i*) **Closure Axiom.** $\forall a, b \in C \Rightarrow a+b \in C$.

[$\because$ *Sum of any two complex numbers is a complex number*]

(*ii*) **Associative Law.** $a+(b+c)=(a+b)+c \ \forall a, b, c \in C$.

(*iii*) **Existence of Identity.** There exists an element $0 \in C$ such that $a+0=a=0+a \ \forall a \in C$.

[**Remember** : 0 is a complex number because $0=0+i(0)$]

(*iv*) **Existence of Inverse.** $\forall a \in C$, there exists an element $-a \in C$ such that $a+(-a)=0=(-a)+a$.

Thus $<C, +>$ is a group.

(*v*) **Commutative Law.** $\forall a, b \in C$, $a+b=b+a$.

Thus $<C, +>$ is an abelian group.

(*vi*) Since the number of complex numbers is infinite,

$\therefore$ C is an infinite set.

Hence $<C, +>$ is an infinite abelian group.

Example 5. (*a*) *Prove that $<N, +>$, where N is a set of natural numbers, is a semi-group and not a group.*

(*b*) *Prove that $<Z^+, +>$, where Z^+ is a set of +ve integers is not a group.*

(*c*) *Is the set of the non-negative integers with operation + a group ? Justify your answer.* [G.N.D.U. 1981]

Sol. (*a*) The system is $<N, +>$, where N is a set of natural numbers and '+' is the binary operation in N.

(*i*) **Closure Axiom.** $\forall a, b \in N \Rightarrow a+b \in N$.

[$\because$ *Sum of any two natural numbers is a natural number*]

(*ii*) **Associative Law.** $a+(b+c)=(a+b)+c \ \forall a, b, c \in N$.

Thus $<N, +>$ is a semi-group.

(*iii*) **Existence of Identity.** Under addition composition, 0 is the identity element

But $0 \notin N$. [$\because$ *0 is not a natural number*]

Thus $<N, +>$ is not a group.

Hence $<N, +>$ is a semi-group and not a group.

(*b*) Same as part (*a*).

(*c*) Please try yourself. **[Ans. Yes]**

Example 6. *Prove that $<N', +>$, where $N'=\{0, 1, 2, 3......\}$ is a semi-group and not a group.*

Sol. The system is $<N', +>$, where $N'=\{0, 1, 2, 3,......\}$ and '+' is the binary operation in N'.

(*i*) **Closure Axiom.** $\forall a, b \in N' \Rightarrow a+b \in N'$.

(*ii*) **Associative Law.** $a+(b+c)=(a+b)+c \ \forall a, b, c \in N'$.

Thus $<N', +>$ is a semi-group.

(*iii*) **Existence of Identity.** There exists an element $0 \in N'$ such that $a+0=a=0+a \ \forall a \in N'$.

(*iv*) **Existence of Inverse.** Under addition composition, $-a$ is the inverse of a.

But $-a \notin N'$. [$\because$ *N' contains no —ve integer*]

Thus $<N', +>$ is not a group.

Hence $<N', +>$ is a semi group and not a group.

Example 7. *Prove that $<N, \times>$, where N is a set of natural numbers is a semi-group with an identity element.*

Sol. The system is $<N, \times>$, where N is a set of natural numbers and '$\times$' is the binary operation in N.

(*i*) **Closure Axiom.** $\forall a, b \in N \Rightarrow a \times b \in N$.

[$\because$ *Product of any two natural numbers is a natural number.*]

(*ii*) **Associative Law.** $a+(b+c)=(a+b)+c \ \forall a, b, c \in N$.

Thus $<N, \times>$ is a semi-group.

(*iv*) **Existence of Identity.** There exists an element $1 \in N$ such that

$$a \times 1 = a = 1 \times a \ \forall \ a \in N.$$

Thus $<N, \times>$ is with an identity element.

Hence $<N, \times>$ is a semi-group with an identity element.

Example 8. *Prove that $<Q, \times>$ is not a group.*

Sol. Please try yourself.

Example 9. *Prove that $<S, \times>$, where $S=\{1\}$ is a finite abelian group.*

Sol. The system is $<S, \times>$, where $S=\{1\}$ and '$\times$' is the binary composition in S.

The element 1 can be repeated again and again.

It is closed, associative law holds.

The identity element 1 exists.

The inverse of 1 is , which is in S.

Also S contains only one element.

Hence $<S, \times>$, where $S=\{1\}$ is a finite abelian group.

Example 10. *Prove that $<S, \times>$, where $S=\{1, -1\}$ is a finite abelian group.*

Sol. Please try yourself.

Example 11. *Prove that $<S, \times>$, where $S=\{1, \omega, \omega^2\}$ when $1, \omega, \omega^2$ are cube roots of unity, is a finite abelian group.*

(Important)

Sol. The system is $<S, \times>$, where

$S=\{1, \omega, \omega^2\}$ while $1, \omega, \omega^2$ are cube roots of unity and thus $\omega^3=1$, and '$\times$' is the binary operation is S.

(*i*) **Closure Axiom.**

Since $1\times\omega=\omega\in S$, $1\times\omega^2=\omega^2\in S$

and $\omega\times\omega^2=\omega^3=1\in S$,

$\therefore$ S is closed under '$\times$'.

(*ii*) **Associative Law.**

$$1\times(\omega\times\omega^2)=1\times(\omega^3)=1\times1=1$$

and $(1\times\omega)\times\omega^2=\omega\times\omega^2=\omega^3=1$.

Thus $1\times(\omega\times\omega^2)=(1\times\omega)\times\omega^2$

$\therefore$ Associative Law holds.

(*iii*) **Existence of Identity.**

Under multiplication 1 works for identity and $1\in S$

$\therefore$ Identity element *i.e.* 1 exists.

(*iv*) **Existence of Inverse.**

Since $1\times1=1=1\times1$, $\therefore$ 1 is the inverse of 1.

Since $\omega\times\omega^2=1=\omega^2\times\omega$, [$\because$ $\omega^3=1$]

$\therefore$ ω^2 is the inverse of ω.

Since $\omega^2\times\omega=1=\omega\times\omega^2$, [$\because$ $\omega^3=1$]

$\therefore$ ω is the inverse of ω^2.

$\therefore$ Inverse of every element of S exists.

Thus $<S, \times>$ is a group.

(*v*) **Commutative Law**

Now $1\times\omega=\omega\times1$, [$\because$ *each* $=\omega$]

$1\times\omega^2=\omega^2\times1$ [$\because$ *each* $=\omega^2$]

and $\omega\times\omega^2=\omega^2\times\omega$ [$\because$ *each* $=\omega^3=1$]

$\therefore$ Commutative Law holds.

Thus $<S, \times>$ is an abelian group.

(*vi*) Since S contains three elements. $\therefore$ S is finite.

Hence $<S, \times>$ is a finite abelian group.

Example 12. *Prove that $<S, \times>$, where S is a set of 4th roots of unity i.e. $S=\{1, -1, i, -i\}$, is a group, where $i^2=-1$.*

Sol. The system is $<S, \times>$, where $S=\{1, -1, i, -i\}$

and '$\times$' is the binary operation in S.

(*i*) **Closure Axiom**

Since $1\times(-1)=-1\in S$, $1\times i=i\in S$,

$1\times(-i)=-i\in S$, $(-1)\times i=-i\in S$,

$(-1)\times(-i)=i\in S$. $i\times(-i)=-i^2=1\in S$.

$\therefore$ S is closed under '$\times$'.

(*ii*) **Associative Law.**

$$1\times(-1\times i)=1\times -i=-i,$$
$$(1\times(-1))\times i=(-1)\times i=-i.$$
$$\therefore \quad 1\times(-1\times i)=(1\times(-1))\times i.$$

Similarly with any other three members of S.

$\therefore$ Associative Law holds.

(*iii*) **Existence of Identity.**

Under multiplication 1 works for identity and $1\in S$.

$\therefore$ Identity element *i.e.* 1 exists.

(*iv*) **Existence of Inverse.**

Since $1\times 1=1=1\times 1$, $\therefore$ 1 is the inverse of 1.

$(-1)\times(-1)=1=(-1)\times(-1)$, $\therefore$ -1 is the inverse of -1.

$i\times(-i)=1=(-i)\times i$, $\therefore$ $-i$ is the inverse of i.

and $-i\times i=1=i\times(-i)$, $\therefore$ i is the inverse of $-i$.

$\therefore$ Inverse of every element of S exists.

Hence $<S, \times>$ is a group.

Example 13. *Prove that n, nth roots of unity form a group under multiplication.* **(V. Important)** **[Pbi. U. 1978]**

Sol. *n*, *n*th roots of unity are given by

$$(1)^{1/n}=(\cos 0+i\sin 0)^{1/n}$$
$$=(\cos 2r\pi+i\sin 2r\pi)^{1/n}$$
$$=\cos\frac{2r\pi}{n}+i\sin\frac{2r\pi}{n}$$
$$=e^{\frac{2ir\pi}{n}},$$

where $r=0, 1, 2, \ldots\ldots\ldots, n-1$.

Now the system is $<S, \times>$,

where $S=\{1, \alpha, \alpha^2, \ldots\ldots\ldots, \alpha^{n-1}\}$

while $\alpha=e^{\frac{2i\pi}{n}}$.

(*i*) **Closure Axiom.**

Let $a, b\in S \Rightarrow a^n=1,\ b^n=1$

$\Rightarrow (ab)^n=a^nb^n=1\times 1=1$

$\Rightarrow ab\in S.$

Thus S is closed under multiplication.

(*ii*) **Associative Law.** Since the multiplication of complex numbers is associative, so the multiplication in S is associative.

(*iii*) **Existence of Identity.**

$1\in S$ such that $1\times a=a\ \forall\ a\in S$

$\Rightarrow$ 1 acts as multiplicative identity.

(*iv*) **Existence of Inverse.**

If $\alpha^r \in S$, then there exists $\alpha^{n-r} \in S$ such that

$$\alpha^{n-r} \times \alpha^r = \alpha^n = 1.$$

$\therefore$ α^{n-r} is the inverse of α^r.

$\therefore$ Inverse of every element of S exists.

Hence $<S, \times>$ is a group under multiplication.

Example 14. *Prove that* $<Q^+, *>$, *where* '$*$' *is the binary operation defined by* $a*b = \frac{ab}{5}$, *is a group.*

Sol. (*i*) **Closure Axiom.**

Let $a, b \in Q^+$, then $a * b = \frac{ab}{5} \in Q^+$.

$$\left[\because \text{ If } a\ b \text{ are +ve rationals, so is } \frac{ab}{5}\right]$$

$\therefore$ Q^+ is closed under ' $*$ '.

(*ii*) **Associative Law.** Let $a, b, c \in Q^+$.

Then $(a*b)*c = \frac{ab}{5} * c = \frac{ab}{5} \cdot \frac{c}{5} = \frac{abc}{25}$

and $a*(b*c) = a* \frac{bc}{5} = \frac{a}{5} \cdot \frac{bc}{5} = \frac{abc}{25}$.

$\therefore$ $(a*b)*c = a*(b*c)$.

$\therefore$ Associative Law holds.

(*iii*) **Existence of Identity.**

$\forall\ a \in Q^+$, $5*a = \frac{5a}{5} = a$,

$$a*5 = \frac{a(5)}{5} = a.$$

$\therefore$ $5*a = a = a*5$.

$\therefore$ 5 is the identity of Q^+, where $5 \in Q^+$.

(*iv*) **Existence of Inverse.**

$\forall\ a \in Q^+$, $a* \frac{25}{a} = \frac{a(25)}{a} \cdot \frac{1}{5} = 5$,

$$\frac{25}{a} * a = \frac{25}{a}(a)\frac{1}{5} = 5.$$

$\therefore$ $a* \frac{25}{a} = 5 = \frac{25}{a} * a$.

$\therefore$ $\frac{25}{a}$ is the inverse of a.

Hence $<Q^+, *>$ is a group

Example 15. *In the set of real numbers R (excluding 1), there is defined a binary operation * for all a, $b \in R-\{1\}$ by $a_* b = a+b-ab$. Is $R-\{1\}$ with * a group?* **(Important)**

Sol. (*i*) **Closure Axiom.**

Let $a, b \in R-\{1\}$, then $a_* b = a+b-ab \in R-\{1\}$.

$\therefore$ $R-\{1\}$ is closed under '*'.

(*ii*) **Associative Law.**

Let $a, b, c \in R-\{1\}$.

Then
$$\begin{aligned}(a_* b)_* c &= (a+b-ab)_* c\\ &= a+b-ab+c-(a+b-ab)c\\ &= a+b-ab+c-ac-bc+abc\\ &= a+b+c-ab-bc-ac+abc\end{aligned}$$

and
$$\begin{aligned}a_*(b_* c) &= a_*(b+c-bc)\\ &= a+(b+c-bc)-a(b+c-bc)\\ &= a+b+c-bc-ab-ac+abc\\ &= a+b+c-ab-bc-ac+abc.\end{aligned}$$

$\therefore$ $(a_* b)_* c = a_*(b_* c)$

$\therefore$ Associative Law holds.

(*iii*) **Existence of Identity.**

$a_* 0 = a+0-a\,.\,0 = a$

and $0_* a = 0+a-0\,.\,a = a.$

Thus $a_* 0 = a = 0_* a$.

$\therefore$ 0 is the identity of $R-\{1\}$, where $0 \in R-\{1\}$.

(*iv*) **Existence of Inverse.**

$\forall a \in R-\{1\}$,

$$a_* \frac{a}{a-1} = a + \frac{a}{a-1} - a\left(\frac{a}{a-1}\right) = 0$$

$$\frac{a}{a-1} {}_* a = \frac{a}{a-1} + a - \frac{a}{a-1}(a) = 0.$$

Thus $a_* \dfrac{a}{a-1} = 0 = \dfrac{a}{a-1} {}_* a$.

$\dfrac{a}{a-1}$ is the inverse of a, where $\dfrac{a}{a-1} \in R-\{1\}$ $(a \neq 1)$.

Thus $R-\{1\}$ is a group.

(*v*) **Commutative Law.**

$a_* b = a+b-ab = b+a-ba = b_* a.$

$\therefore$ Commutative Law holds.

Thus $R-\{1\}$ is an abelian group.

(*vi*) $R-\{1\}$ contains an infinite number of elements.

Hence $R-\{1\}$ is an infinite abelian group.

Example 16. *Prove that* $<Q, *>$, *where* '$*$' *is the binary operation defined by* $a*b=ab+a+b$ *is a group.*

Sol. Please try yourself.

Example 17. *Let* R_2 *be a set of matrices of the form* $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, *where* a, b, c, d *are real and* $ad-bc\neq 0$. *Prove that* R_2 *is a group under matrix multiplication.* **(V. Important)**
[Pbi. U. 1976]

Sol. (*i*) **Closure Axiom**

Let $A=\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $B=\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$.

Thus $A, B \in R_2$.

Now $$AB=\begin{bmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{bmatrix} \in R_2$$
$[\because \ |A|\neq 0, \ |B|\neq 0, \ |AB|\neq 0]$

(*ii*) **Associative Law**

$(A.B).C=A.(B.C)$
[$\because$ *Matrix multiplication is associative*]

(*iii*) **Existence of Identity**

$I=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ acts as multiplicative identity because

$A\times I=I\times A$.

(*iv*) **Existence of Inverse**

A^{-1} exists because $|A|\neq 0$ and belongs to R_2.
Hence R_2 is a group under multiplication.

Example 18. *Prove that* $J_n=\{0, 1, 2, \ldots\ldots, n-1\}$ *form an abelian group under the composition addition* $\equiv$ *(mod n).* **(Important)**

Sol. $\forall \ a, b \in J_n, \quad a+b=nq+r$

$\Rightarrow \quad (a+b)-r=nq$

$\Rightarrow \quad a+b\equiv r \pmod n$, where $0\leqslant r<n$.

(*i*) **Closure Axiom.** It is closed under the given composition.

(*ii*) **Associative Law.** $(a+b)+c\equiv[a+(b+c)] \pmod n$.

(*iii*) **Existence of Identity element.**

Here 0 acts as identity element.
[$\because$ $a+0\equiv a$ (*mod n*) *because* $n \mid a-a$]

(*iv*) **Existence of Inverse.**

The inverse of 0 is 0. [$\because$ $0+0\equiv 0$ (*mod n*)]
Also the inverse of k is $n-k$
[$\because$ $k+(n-k)\equiv 0$ (*mod n*), $k\neq 0$ *and* $n-k\in J_n$]

(v) **Commutative Law.** $(a+b) \equiv (b+a) \pmod{n}$.

Hence J_n is an abelian group.

Example 19. *Check whether the following are groups or not? Give reasons :*

(i) *Define '$*$' on Z (set of integers) by* $a * b = ab$.

(ii) *Define '$*$' on Z (set of integers) by* $a * b = a - b$.

(iii) *Define '$*$' on R^+ (set of +ve reals) by* $a * b = ab$.

(iv) *Define '$*$' on Q (set of rationals) by* $a * b = ab$.

Sol. (i) No. [$\because$ Inverse does not exist]

(ii) No. [$\because$ '$*$' is not associative]

(iii) Yes.

(iv) No. [$\because$ *Inverse does not exist*]

ELEMENTARY PROPERTIES

An Important Note. When G is a group with respect to binary operation $*$, we shall simply write ab instead of $a*b$, where a and b are elements in G.

Property I. Cancellation laws hold in a group.

If G is a group, for all $a, x, y \in G$,

(i) $ax = ay \Rightarrow x = y$ **[Left Cancellation Law]**

(ii) $xa = ya \Rightarrow x = y$ **[Right Cancellation Law]**

Proof. (i) Given $ax = ay$

Let a^{-1} be the inverse of a in G.

Then $ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay)$

[*Multiplying both sides by a^{-1} on the left*]

$\Rightarrow (a^{-1}a)x = (a^{-1}a)y$ [*By Associative Law*]

$\Rightarrow ex = ey$ [$\because a^{-1}a = e$]

$\Rightarrow x = y.$ [$\because ex = x \ \forall \ x \in G$]

(ii) Given $xa = ya$.

Let a^{-1} be the inverse of a in G.

Then $xa = ya \Rightarrow (xa)a^{-1} = (ya)a^{-1}$

[*Multiplying both sides by a^{-1} on the right*]

$\Rightarrow x(aa^{-1}) = y(aa^{-1})$ [*By Associative Law*]

$\Rightarrow xe = ye$ [$\because aa^{-1} = e$]

$\Rightarrow x = y.$ [$\because xe = x \ \forall \ x \in G$]

Property II. *Given two elements a, b of the group G, there exist unique elements $x, y \in G$ such that*

$$ax = b \text{ and } ya = b.$$

Proof. We have $ax = b$

$\Rightarrow a^{-1}(ax) = a^{-1}b$

[*Multiplying both sides by a^{-1} on the left*]

$\Rightarrow \quad (a^{-1}a)x = a^{-1}b$ [*By Associative Law*]

$\Rightarrow \quad ex = a^{-1}b$ [$\because \; a^{-1}a = e$]

$\Rightarrow \quad x = a^{-1}b$ [$\because \; ex = e \; \forall \; x \in G$]

Again $\quad ya = b$

$\Rightarrow \quad (ya)\,a^{-1} = ba^{-1}$

[*Multiplying both sides by* a^{-1} *on the right*]

$\Rightarrow \quad y(aa^{-1}) = ba^{-1}$ [*By Associative Law*]

$\Rightarrow \quad ye = ba^{-1}$ [$\because \; aa^{-1} = e$]

$\Rightarrow \quad y = ba^{-1}$ [$\because \; ye = y \; \forall \; y \in G$]

Now $\quad a \in G \Rightarrow a^{-1} \in G$ [$\because$ *G is a group*]

Now $\quad a^{-1} \in G, \; b \in G \Rightarrow a^{-1}b \in G$ and $ba^{-1} \in G$

[*By Closure Axiom*]

Hence x and y exist.

Uniqueness.

If possible, let there be two solutions $x_1, \; x_2$ of the equation $ax = b$, then $ax_1 = b$ and $ax_2 = b$.

$\therefore \quad ax_1 = ax_2$ [$\because$ *each* $= b$]

$\Rightarrow \quad x_1 = x_2$ [*By Left Cancellation Law*]

Hence the solution of $ax = b$ is unique.

Similarly the solution of $ya = b$ is unique.

Another Form.

If G is a group and if a and b are elements of G, then the equations $ax = b$ and $ya = b$ have unique solutions in G.

Property III. Reversal Law.

The inverse of the product of two elements of a group is the product of their inverses in the reverse order i.e.

$$(ab)^{-1} = b^{-1}a^{-1} \; \forall \; a, b \in G.$$

Proof. Let a, b be two elements of the group G.

Let a^{-1}, b^{-1} be their respective inverses.

Now $\quad (ab)(b^{-1}a^{-1}) = a(bb^{-1})\,a^{-1} = ae\,a^{-1} = e$

and $\quad (b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e.$

Thus $\quad (ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})(ab).$

Hence $b^{-1}a^{-1}$ is the inverse of ab

i.e. $\quad (ab)^{-1} = b^{-1}a^{-1}.$

Generalisation. $(a_1a_2 \ldots\ldots a_n)^{-1} = a_n^{-1}\,a_{n-1}^{-1} + \ldots\ldots a_2^{-1}\,a_1^{-1}.$

Proof. Let $\quad n = 2.$

$\therefore \quad (a_1\,a_2)^{-1} = a_2^{-1}\,a_1^{-1}$ [*Proved above*]

Thus the result is true when $n = 2$.

Let us assume that the result is true for $n = k$.

$\therefore \quad (a_1\,a_2 \ldots\ldots a_k)^{-1} = a_k^{-1}\,a_{k-1}^{-1} \ldots\ldots a_2^{-1}\,a_1^{-1}.$

We shall prove that the result is true for $n=k+1$.

Now $(a_1 a_2 \ldots\ldots a_k\, a_{k+1})^{-1}=(a_1 a_2 \ldots\ldots a_k\, a_{k+1})^{-1}$

$$=a_{k+1}^{-1}\,(a_1a_2\ldots\ldots a_k)^{-1}$$
$$=a_{k+1}^{-1}\,a_k^{-1}\ldots\ldots a_2^{-1}\,a_1^{-1}.$$

Thus the result is true when $n=k+1$.

Hence the result is true for all n.

Property IV. Prove that the identity element in a group is unique.

Proof. If possible, let e, e' be two identity elements in a group G.

Now regarding e as identity, we have :—

$ee'=e'$ ...(1) [$\because$ *e is identity*, $\therefore$ $ex=x\ \forall\ x \in G$]

Again regarding e' as identity, we have

$ee'=e$ ...(2) [$\because$ *e' is identity*, $\therefore$ $xe'=x \forall x \in G$]

From (1) and (2), $e'=e$ [$\because$ *each*$=ee'$]

Hence the identity element in a group is unique.

Property V. Prove that inverse of an element in a group is unique. (Important) [*Pbi. U. 1977.*]

Proof. If possible, let a', a'' be two inverses of a in G.

Since a' is the inverse of a, $\therefore$ $a'a=aa'=e$ ...(1)

Since a'' is the inverse of a, $\therefore$ $a''a=aa''=e$ ...(2)

From (1) and (2), $aa'=aa''$ [$\because$ *each*$=e$]

$\Rightarrow$ $a'=a''$ [*By Left Cancellation Law*]

Also from (1) and (2), $a'a=a''a$

$\Rightarrow$ $a'=a''$ [*By Right Cancellation Law*]

Hence the inverse of an element in a group is unique.

Property VI. Prove that the inverse of the inverse of an element in a group is the element itself.

i.e. $(a^{-1})^{-1}=a\ \forall\ a \in G$.

Proof. Let $a \in G \Rightarrow a^{-1} \in G$.

Now $a^{-1}(a^{-1})^{-1}=e$

$$=a^{-1}\,a$$

$\Rightarrow$ $(a^{-1})^{-1}=a$ [*By Left Cancellation Law*]

Also $(a^{-1})^{-1}\,a^{-1}=e$

$$=a\,a^{-1}$$

$\Rightarrow$ $(a^{-1})^{-1}=a$ [*By Right Cancellation Law*]

Hence $(a^{-1})^{-1}=a$.

Property VII. A finite set G with a closed associative binary operation is a group if and only if the left and right cancellation laws hold in G.

Proof. I, If G is a group, then left and right cancellation laws hold. [This has been proved in property I]

II. Let G consist of n elements; say

$$a_1, a_2, \ldots\ldots\ldots a_n \qquad \ldots(A)$$

Consider the set having elements

$$aa_1, aa_2, \ldots\ldots aa_n \qquad \ldots(B),$$

where a is an element of G.

Every element of list (B) belongs to *G* [$\because$ *G is closed w.r.t.* *]

No two elements of list (B) are same.

For if $aa_i = aa_j \Rightarrow a_i = a_j$ [*By Left Cancellation Law*]

This is impossible because $a_i \neq a_j$

Hence G consists exactly the elements

$$aa_1, aa_2, \ldots\ldots, aa_n$$

Stated otherwise, if b be an element of G, we must have

$$b = aa_i \text{ for some } i.$$

Hence the equation $ax = b$ has a solution in G.

Similarly the equation $ya = b$ has a solution in G.

Hence G is a group. [*By Property II, Another Form*]

Integral Powers and Multiples of an Element of a Group

(*a*) **Integral Powers.** Let '*' be the binary operation in the group G.

Then
$$a * a = a.a = a^2$$
$$a * a * a = a^2.a = a^3$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Similarly $a * a \ldots\ldots\ldots$ to m factors $= a^m$, where m is a +ve integer.

Also
$$a^0 = e$$
And
$$a^{-1} = a^{-1}$$
$$a^{-2} = (a^{-1})^2$$
$$\ldots\ldots\ldots\ldots$$
$$a^{-m} = (a^{-1})^m$$

(*b*) **Multiples.** Let '+' be the binary operation in the group G

Then
$$a + a = 2a$$
$$a + a + a = 3a$$
$$\ldots\ldots\ldots\ldots$$
$$a + a + \ldots\ldots \text{to } m \text{ terms} = ma$$

Also
$$0a = 0$$
And
$$(-1)a = -a$$
$$-2a = 2(-a)$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$-ma = m(-a)$$

Example 20. *Prove that if $a^2=a$, $a\in G$, then $a=e$.*

Sol. We have : $a^2=a \Rightarrow aa=a$

$\Rightarrow aa=ae$ [$\because$ $ae=a$]

$\Rightarrow a=e$ [*By Left Cancellation Law*]

Hence the result.

Example 21. *Show that every group G with identity e such that $x^2=e$ for all $x\in G$ is abelian.*

Sol. Let $a, b\in G$, $\therefore$ $ab\in G$ [$\because$ *G is closed*]

Now $(ab)^2=e$ [*Given*]

$\Rightarrow$ $(ab)(ab)=e$

$\Rightarrow$ $a(ba)b=e$ [*By Associative Law*]

$\Rightarrow$ $(a(ba)b)b=eb$ [*Multiplying by b on the right*]

$\Rightarrow$ $a(a(ba)b)b=aeb$ [*Multiplying by a on the left*]

$\Rightarrow$ $(aa)(ba)(bb)=(ae)b$

$\Rightarrow$ $a^2(ba)b^2=ab$

$\Rightarrow$ $e(ba)e=ab$ [$\because$ $a^2=b^2=e$]

$\Rightarrow$ $ba=ab$

$\Rightarrow$ G is abelian.

Example 22. *Prove that a group G is abelian if*

$b^{-1}a^{-1}ba=e$ for all $a, b\in G$.

Sol. We have : $b^{-1}a^{-1}ba=e\ \forall a,b\in G$ [*Given*]

$\Rightarrow$ $bb^{-1}a^{-1}ba=be$ [*Multiplying by b an the left*]

$\Rightarrow$ $ea^{-1}ba=b$

$\Rightarrow$ $a^{-1}ba=b$

$\Rightarrow$ $aa^{-1}ba=ab$ [*Multiplying by a on the left*]

$\Rightarrow$ $eba=ab$

$\Rightarrow$ $ba=ab$

$\Rightarrow$ G is abelian.

Example 23. *Show that if a, b are any two elements of a group G, then $(ab)^2=a^2b^2$ if and only if G is abelian.*

(V. Important) **[Pbi. U. 1977]**

Sol. **Given** : G is abelian.

To Prove : $(ab)^2=a^2b^2$.

Now $(ab)^2=(ab)(ab)$

$=a(ba)b$ [*By Associative Law*]

$=a(ab)b$ [*ab=ba because G is abelian*]

$=(aa)(bb)$ [*By Associative Law*]

$=a^2b^2$.

Conversely : Given $(ab)^2=a^2b^2$.

To Prove : G is abelian.

Now $(ab)^2=a^2b^2$

$\Rightarrow$ $(ab)(ab)=(aa)(bb)$

$\Rightarrow$ $a(ba)b=a(ab)b$ [*By Associative Law*]

$\Rightarrow$ $(ba)b=(ab)b$ [*By Left Cancellation Law*]

$\Rightarrow$ $ba=ab$ [*By Right Cancellation Law*]

$\Rightarrow$ G is abelian.

Example 24. *If G is an abelian group, then for all $a, b \in G$,* $(ab)^n=a^nb^n$. **(V. Important) [Pbi. U. 1978]**

Sol. *If* $n=1$, $(ab)^1=ab=a^1b^1$.

Thus the result is true for $n=1$.

Let us assume that the result is true for $n=k$.

Then $(ab)^k=a^kb^k$.

Now
$$
\begin{aligned}
(ab)^{k+1}&=(ab)^k(ab)\\
&=a^kb^k\,ab\\
&=a^k(b^ka)b && \text{[By Associative Law]}\\
&=a^k(ab^k)b && [\because G \text{ is abelian } b^ka=ab^k]\\
&=a^ka\,b^kb\\
&=a^{k+1}\,b^{k+1}
\end{aligned}
$$

Thus the result is true for $n=k+1$.

Hence, by mathematical induction, the result is true for all n.

Example 25. *If G is a group and e is the identity, prove that* $(l\,ab^{-1})^n=ba^nb^{-1}$.

Sol. *If* $n=1$, $(bab^{-1})^1=bab^{-1}$
$=ba^1b^{-1}$.

Thus the result is true for $n=1$.

Let us assume that the result is true for $n=k$.

Then $(bab^{-1})^k=ba^k\,b^{-1}$.

Now
$$
\begin{aligned}
(bab^{-1})^{k+1}&=(bab^{-1})^k(bab^{-1})\\
&=(ba^kb^{-1})(bab^{-1})\\
&=ba^k(b^{-1}b)ab^{-1}\\
&=b(a^kea)b^{-1}\\
&=b(a^ka)b^{-1}\\
&=ba^{k+1}b^{-1}
\end{aligned}
$$

Thus the result is true for $n=k+1$.

Hence, by mathematical induction, the result is true for all n.

Example 26. *If G is a group and e is the identity, prove that* $e^n=e$.

Sol. Please try yourself.

Example 27. *Prove that if every element of the group G is its own inverse, then G is abelian.*

Sol. Let a, b be any two elements of G.

Then ab is also an element of G [$\because$ *G is closed*]

By the question, $(ab)^{-1}=ab$

$\Rightarrow$ $b^{-1}a^{-1}=ab$

$\Rightarrow$ $ba=ab$ [$\because$ $b^{-1}=b$ *and* $a^{-1}=a$]

$\Rightarrow$ G is abelian.

Example 28. *If G is a group and $2a=0$ for all $a \in G$, then G is abelian.*

Sol. [Here '+' is the binary operation and '0' is the identity]

We have : $2a=0 \quad \forall\ a \in G$

$\Rightarrow$ $a+a=a+(-a)$

$\Rightarrow$ $a=-a$ [*By Left Cancellation Law*]

Similarly $\forall\ b \in G$, $b=-b$.

Now $\forall a, b \in G$, $a+b \in G$ [$\because$ *G is closed*]

$\Rightarrow$ $2(a+b)=0$ [*By the question*]

$\Rightarrow$ $a+b=-(a+b)$ [*By above*]

$\Rightarrow$ $a+b=-b-a$

$\Rightarrow$ $a+b=b+a$

$\Rightarrow$ G is abelian.

Example 29. *If G is a group of even order, prove that it has an element $a \neq e$ satisfying $a^2=e$.*

Sol. In a group every element possesses its inverse and the identity element e is its own inverse.

Since the number of elements in G is even, [*Given*]

$\therefore$ there is at least one more element of G which is its own inverse.

Hence in G, there is an element $a \neq e$ such that

$$a=a^{-1} \Rightarrow aa=aa^{-1}$$
$$\Rightarrow a^2=e.$$

SUB-GROUPS [*G.N.D.U. 1979*]

(*i*) **Definition.** *Let G be a group under a binary composition '*' and H a non-empty subset of G. The n H is called a sub-group of G if H is a group in itself under the same binary composition.*

(*ii*) **Complex.** *Any (non-empty) sub-set of a group is a complex.*

☞ **Remark : Every sub-group of G is a complex of G but every complex may not be a sub-group.**

(*iii*) **Trivial or Improper sub-groups.**

Since every set is a subset of itself, therefore, if G is a group, then G itself is a sub-group of G.

Also a subset consisting of identity alone will always be a sub-group of the group G.

These two sub-groups of G are called **trivial** or **improper sub-groups** of G.

(*iv*) **Proper sub-group.** If there is any other sub-group of G except the group itself and the group containing identity element alone, it is called **proper sub-group.**

Illustrations :

(I) $<R, +>$ is a sub-group of $<C, +>$.

[$\because$ *Every real number is a complex number*]

(II) $<Q, +>$ is a sub-group of $<R, +>$.

[$\because$ *Every rational number is a real number*]

(III) $<N, +>$ is not a sub-group.

[$\because$ *0, which works for identity, is not a rational number*]

(IV) $<R^+, \times>$ is a sub-group of $<R, \times>$.

[$\because$ *Every +ve real number is a real number*]

(V) The set E of even integers is a subgroup of the **additive** group of integers.

(VI) Let G be a group of integers under **addition** ; H the subset consisting of all the multiples of 5. Then H is a sub-group of G.

(VII) Let $G=\{1, -1, i, -i\}$ be the group of 4th roots of unity under **multiplication**. Then $H=\{1, -1\}$ is a subgroup of G.

(VIII) Let G be the multiplicative group of all non-singular matrices over complex numbers.

Let H be the set of following eight matrices :

$$\pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Clearly $H \subseteq G$. Also H is a subgroup under multiplication.

Hence H is a subgroup of G.

Note : The above illustrations can be verified by proceeding as in Examples on Groups.

Example 30. *Consider the group $J_6=\{0, 1, 2, 3, 4, 5\}$ under the composition addition$\equiv$(mod 6).*

Prove that

(*i*) *$H_1=\{0, 3\}$ is a sub-group of J_6.*

(*ii*) *$H_2=\{2, 3, 5\}$ is only a complex of J_6.*

(*iii*) *$H_3=\{0, 2, 4\}$ is a subgroup of J_6.* **(Important)**

Sol. (*i*) Here $J_6=\{0, 1, 2, 3, 4, 5\}$ and $H_1=\{0, 3\}$, composition is addition$\equiv$(mod 6).

(I) **Closure Axiom.** H_1 is closed under given composition.

[$\because$ $0+3=3 \pmod 6$ and $3 \in H_1$]

(II) **Associative Law.** It is obvious.

(III) **Existence of Identity element.**

Here 0 acts as an identity element and $0 \in H_2$.

[$\because$ $0+0 \equiv 0 \pmod 3$ and $3+0 \equiv 3 \pmod 3$]

(IV) **Existence of Inverse.**

The inverse of 0 is 0. [$\because$ $0+0 \equiv 0 \pmod 6$]

The inverse of 3 is 3. [$\because$ $3+3=6 \equiv 0 \pmod 6$]

Thus H_1 is a group in itself.

Also $H_1 \subset J_6$.

Hence H_1 is a sub-group of J_6.

(*ii*) Here $H_2=\{2,3,5\}$.

This is not closed.

[$\because$ $5+2=7 \equiv 1 \pmod 6$ and $1 \notin H_2$]

$\therefore$ H_2 is not a group.

Hence H_2 is only a complex of J_6.

(*iii*) Here $H_3=\{0,2,4\}$.

(I) **Closure Axiom.** H_3 is closed under given composition.

[$\because$ $0+2 \equiv 2 \pmod 6$ and $2 \in H_3$,

$0+4 \equiv 4 \pmod 6$ and $4 \in H_3$,

and $2+4=6 \equiv 0 \pmod 6$ and $0 \in H_3$]

(II) **Associative Law.**

$$(0+2)+4=2+4=6 \equiv 0 \pmod 6$$

$$0+(2+4)=0+6=6 \equiv 0 \pmod 6.$$

Thus $(0+2)+4=0+(2+4)$ under composition addition $\equiv \pmod 6$.

(III) **Existence of Identity element.**

Here 0 acts as an identity element and $0 \in H_3$.

[$\because$ $0+0 \equiv 0 \pmod 6$, $2+0 \equiv 2 \pmod 6$, $4+0 \equiv 4 \pmod 6$]

(IV) **Existence of Inverse.**

The inverse of 0 is 0. [$\because$ $0+0 \equiv 0 \pmod 6$]

The inverse of 2 is 4, and $4 \in H_3$. [$\because$ $2+4=6 \equiv 0 \pmod 6$]

The inverse of 4 is 2, and $2 \in H_3$. [$\because$ $4+2=6 \equiv 0 \pmod 6$]

Thus inverses of all elements exist.

Thus H_3 is a group in itself.

Also $H_3 \subset J_6$.

Hence H_3 is a sub-group of J_6.

CRITERIONS FOR SUB-GROUPS

Theorem I. *A non-empty set H of a group G is a sub-group of G if and only if* $a, b \in H \Rightarrow ab^{-1} \in H$. **[V. Imp.]**

Proof. Given : H is a sub-group of G.

To Prove : $a, b \in H \Rightarrow ab^{-1} \in H$.

Since H is a sub-group of G, $b \in H \Rightarrow b^{-1} \in H$.

$\therefore\ a \in H, b^{-1} \in H \Rightarrow ab^{-1} \in H$ [$\because$ *H is closed*]

Converse : Given : $a, b \in H \Rightarrow ab^{-1} \in H$.

To Prove : H is a subgroup of G.

Since $a \in H, a \in H \Rightarrow aa^{-1} \in H$ [*Putting* $b=a$]

$\Rightarrow e \in H$.

Thus identity element exists in H.

Also $e \in H, a \in H \Rightarrow ea^{-1} \in H$

[*By the given condition*]

$\Rightarrow a^{-1} \in H$.

Thus inverse of each element belongs to H.

Hence H is a sub-group of G.

Note : The identity of a group is also the identity of its sub-groups.

Theorem II. *Let G be a group and H be a finite non-empty subset of G. Then H is a sub-group of G if and only if* $ab \in H$ *for all* $a, b \in H$. **(V. Important) [Pbi.U. 1975]**

Proof. Given : H is a finite subgroup of G.

To Prove : $\forall\ a, b \in H \Rightarrow ab \in H$.

Since H is a subgroup,

$\therefore$ H is a group in itself.

$\therefore\ \forall\ a, b \in H \Rightarrow ab \in H$. [$\because$ *H is closed*]

Converse : Given : $\forall\ a, b \in H \Rightarrow ab \in H$ and H is finite.

To Prove : H is a subgroup of G.

$$a \in H \Rightarrow a^2 = aa \in H,$$
$$a^3 = a^2 a \in H$$
$$\cdots\cdots\cdots$$
$$a^n \in H \quad [\because \textit{ H is closed}]$$
$$\cdots\cdots\cdots$$

Thus the infinite collection of elements $a, a^2, a^3, \ldots\ldots, a^n, \ldots\ldots$ must all fit into H, which is a finite subset of G.

$\therefore$ There must be repetitions in this collection of elements, i.e. for some integers r and s, $a^r = a^s$, where $r > s$

$\Rightarrow a^{r-s} = a^0$ [*By Cancellation Law*]

$= e$ ...(1)

But $r - s = m$, a +ve integer [$\because$ *r and s are +ve integers and* $r > s$]

$\therefore\ a^m = e$

$\Rightarrow e \in H$. [$\because$ *Every power of* $a \in H$]

Thus identity element exists.

Now $a^{r-s-1} \in H$ [$\because$ *Every power of* $a \in H$]

$\Rightarrow \quad a^{r-s} \cdot a^{-1} \in H$

$\Rightarrow \quad e\, a^{-1} \in H$ [*From* (*1*)]

$\Rightarrow \quad a^{-1} \in H.$

Thus inverse element of every element exists.

Hence H is a sub-group of G.

Theorem III. (*a*) *The intersection of two sub-groups is also a subgroup.* **[G.N.D.U. 1981 ; Pbi. U. 1974]**

Proof. Let H_1 and H_2 be two sub-groups of G.

Since H_1 is a sub-group,

$\therefore \quad a \in H_1, b \in H_1 \quad \Rightarrow \quad ab^{-1} \in H_1$ ...(1)

Since H_2 is a sub-group,

$\therefore \quad a \in H_2, b \in H_2 \quad \Rightarrow \quad ab^{-1} \in H_2$ ...(2)

Now $a \in H_1, a \in H_2 \quad \Rightarrow \quad a \in H_1 \cap H_2$

and $\quad b \in H_1, b \in H_2 \quad \Rightarrow \quad b \in H_1 \cap H_2.$

From (1) and (2), $\quad ab^{-1} \in H_1, ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2.$

Thus if $a, b \in H_1 \cap H_2$, then $ab^{-1} \in H_1 \cap H_2$.

Hence, by Theorem I, $H_1 \cap H_2$ is a sub-group of G.

Caution *The union of two sub-groups may or may not be a sub-group.*

For Example : *Consider the group* $J_6 = \{0, 1, 2, 3, 4, 5\}$ *under composition addition* $\equiv$ *(mod 6).*

Here $H_1 = \{0, 3\}$ *and* $H_2 = \{0, 2, 4\}$ *are its subgroups.*

Here $H_1 \cap H_2 = \{0\}$, which is definitely a subgroup of J_6.

And $\quad H_1 \cup H_2 = \{0, 2, 3, 4\}$ is not a subgroup of J_6.

[$\because \quad 3+4=7 \equiv 1 \pmod 6$ and $1 \notin H_1 \cup H_2$]

(*b*) **Generalisation.** *If* $H_1, H_2, \ldots\ldots, H_n$ *are sub-groups of* G, *then* $\bigcap_{i=1}^{n} H_i$ *is also a sub-group of* G.

Proof. Let $H_1, H_2, \ldots\ldots, H_n$ be n subgroups of G.

Since H_i is a subgroup,

$\therefore \quad a \in H_i, b \in H_i \quad \Rightarrow \quad ab^{-1} \in H_i.$

Also $\quad a \in H_1, a \in H_2, \ldots\ldots, a \in H_n \quad \Rightarrow \quad a \in \bigcap_{i=1}^{n} H_i$

$\quad b \in H_1, b \in H_2, \ldots\ldots, b \in H_n \quad \Rightarrow \quad b \in \bigcap_{i=1}^{n} H_i$

If $a, b \in \bigcap_{i=1}^{n} H_i$, then $ab^{-1} \in \bigcap_{i=1}^{n} H_i$

Hence $\bigcap_{i=1}^{n} H_i$ is a sub-group of G.

COSETS

(*i*) **Right Coset.** *Let G be a group and H be a sub-group of G. Then for any $a \in G$, the set $Ha = \{ha \mid h \in H\}$ is called a right coset of H determined by a.*

For Example :

Let $\quad G = \{-1, 1, -i, i\}$ and $H = \{-1, 1\}$,

then $\quad H_i = \{-i, i\}$, $H \times 1 = \{-1, 1\}$, $H \times -1 = \{1, -1\}$

and $\quad H \times -i = \{i, -i\}$.

Thus there are only two right cosets H and H_i of H in G.

(*ii*) **Left Coset.** *Let G be a group and H be a subgroup of G. Then for any $a \in G$, the set $aH = \{ah \mid h \in H\}$ is called a left coset of H determined by a.*

For Example :

Let $\quad G = \{-1, 1, -i, i\}$ and $H = \{-1, 1\}$,

then $\quad iH = \{-i, i\}$, $1 \times H = \{-1, 1\}$, $-1 \times H = \{1, -1\}$

and $\quad -i \times H = \{i, -i\}$.

Thus there are only two left cosets H and iH of H in G.

(*iii*) **Index.** *Let H be a subgroup of G. Then the index of H in G is the number of distinct right cosets of H in G.*

This is denoted by $i_G(H)$ or $[G : H]$.

For Example :

Let $G = \{-1, 1, -i, i\}$ and $H = \{-1, 1\}$.

Then index of H in G is 2.

[$\because$ *There are only two right (or left) cosets af H in G viz. H and H_i*]

THEOREMS

Theorem I. *Let H be a sub-group of a group G. Then any two right cosets of H are either disjoint or identical i.e. either $H_a \cap H_b = \phi$ or $H_a = H_b$.*

Proof Let H be a sub-group of G.

Let H_a, H_b be two right cosets of the subgroup H of G, where $a, b \in G$.

To cases arise :

Case I. *When H_a and H_b have no common element.*

In this case H_a and H_b are disjoint.

Hence $H_a \cap H_b = \phi$.

Case II. *When H_b and H_b have a common element.*

Let c be the common element of H_a and H_b.

Thus $c \in H_a$, $C \in H_b \Rightarrow c \in H_a \cap H_b$.

Then $\exists$ elements h_1 and h_2 such that $c = h_1 a$ and $c = h_2 b$.

$\Rightarrow \quad h_1 a = h_2\, b \qquad$ [$\because$ *each* $= c$]

$\Rightarrow \quad h_1 a\, b^{-1} = h_2 b\, b^{-1} \qquad$ [*Post-multiplying by* b^{-1}]

$\Rightarrow \quad h_1 a\, b^{-1} = h_2 e$

$\Rightarrow \quad h_1 a\, b^{-1} = h_2$

$\Rightarrow \quad H(h_1 ab^{-1}) = H_{h_2}$

$\Rightarrow \quad H(h_1 ab^{-1}) = H \qquad$ [$\because$ $Hh_2 = H$ *as* $h_2 \in H$]

$\Rightarrow \quad Hh_1(ab^{-1}) = H$

$\Rightarrow \quad H(ab^{-1}) = H \qquad$ [$\because$ $Hh_1 = H$ *as* $h_1 \in H$]

$\Rightarrow \quad Hab^{-1}\, b = Hb \qquad$ [*Post-multiplying by* b]

$\Rightarrow \quad H_a = H_b$

Hence if H_a, H_b are not disjoint, then H_a and H_b are identical.

Theorem II. *Let H be a sub-group of a group G. Then all cosets of H have the same number of elements and every element of G is in some right coset of H.*

Proof. (*i*) Consider the mapping

$\lambda_a : H \to H_a$ given by $\lambda_a(h) = ha$.

The mapping is onto.

Because if $h_a \in H_a$,

$\exists\, h \in H$ such that $\lambda_a\,(b) = h_a$.

The mapping is 1—1.

Because $\lambda_a(h_1) = \lambda_a(h_2)$, where $h_1, h_2 \in H$

$\Rightarrow \quad h_1 a = h_2 a$

$\Rightarrow \quad h_1 = h_2 \qquad$ [*By Right Cancellation Law*]

Thus λ_a maps H one-one and onto H_a.

Hence every right coset has the same number of elements.

(*ii*) $e \in H \qquad$ [$\because$ *H is a sub-group*]

$\Rightarrow \quad a = ea$, where a is any element of G

$\Rightarrow \quad a \in H_a$

Hence every element of G is in some right coset of H in G.

Example 31. *Show that there is one-one correspondence between the set of left cosets of H in G and the set of right cosets of H in G.*

Sol. Consider the mapping φ ; which maps the set of all left cosets into the set of all right cosets given by

$$\varphi(aH) = Ha^{-1} \qquad \forall a \in G.$$

To Prove. *ϕ is well-defined.*

Proof. We have : $aH=bH$

$\Rightarrow$ $a, b\in H$

$\Rightarrow$ $a, b^{-1}\in H$ [$\because$ *H is a sub-group*]

$\Rightarrow$ $b^{-1}a\in H$ [$\because$ *H is closed*]

$\Rightarrow$ $(b^{-1}a)^{-1}\in H$ [$\because$ *Inverse exists*]

$\Rightarrow$ $a^{-1}(b^{-1})^{-1}\in H$ [$\because$ $(ab)^{-1}=b^{-1}a^{-1}$, *where* $a, b\in H$]

$\Rightarrow$ $a^{-1}b\in H$ [$\because$ $(b^{-1})^{-1}=b$]

$\Rightarrow$ $Ha^{-1}b=H$ [$\because$ *If* $h\in H$, *the* $Hh=H$]

$\Rightarrow$ $Ha^{-1}bb^{-1}=Hb^{-1}$ [*Post-multiplying by* b^{-1}]

$\Rightarrow$ $Ha^{-1}e=Hb^{-1}$ [$\because$ $bb^{-1}=e$]

$\Rightarrow$ $Ha^{-1}=Hb^{-1}$

$\Rightarrow$ $\varphi(aH)=\varphi(bH)$

Thus φ is well defined.

To Prove. *φ is one-one.*

Proof. We have :

$\varphi(aH)=\varphi(bH)$

$\Rightarrow$ $Ha^{-1}=Hb^{-1}$

$a^{-1}\in Hb^{-1}$

$\Rightarrow$ $a^{-1}b\in H$

$\Rightarrow$ $a^{-1}b\in H$

$\Rightarrow$ $(a^{-1}b)^{-1}\in H$ [$\because$ *Inverse exists*]

$\Rightarrow$ $b^{-1}(a^{-1})^{-1}\in H$ [$\because$ $(ab)^{-1}=b^{-1}a^{-1}$]

$\Rightarrow$ $b^{-1}a\in H$ [$\because$ $(a^{-1})^{-1}=a$]

$\Rightarrow$ $b^{-1}aH=H$

$\Rightarrow$ $bb^{-1}aH=bH$ [*Pre-multiplying by b*]

$\Rightarrow$ $eaH=bH$ [$\because$ $bb^{-1}=e$]

$\Rightarrow$ $aH=bH$

Thus φ is one-one.

To Prove. *φ is onto.*

Proof. Let Ha be any right coset.

Then $a^{-1}H$ is a left coset.

Also $\varphi(a^{-1}H)=H(a^{-1})^{-1}=Ha$.

Thus each right coset is the φ—image of the left coset of $a^{-1}H$.

Thus φ is onto.

Hence the result.

Example 32. *Let G be a group of integers under addition, H_n the sub group consisting of all multiples of a fixed integer n in G. Find the index of H_n in G and write all the cosets of H_n in G.*

Sol. Let $G=\{......-3, -2, -1, 0, 1, 2, 3,......\}$

Then $H_n=\{......-3n, -2n, -n, 0, n, 2n, 3n,......\}$

$$H_1 = \{......-3, -2, -1, 0, 1, 2, 3,......\}$$
$$H_2 = \{......-6, -4, -2, 0, 2, 4, 6,......\}; \text{ etc.}$$

Hence index of H_n in $G = n$.

LAGRANGE'S THEOREM (V. Imp.)

Statement. *The order of every sub-group of a finite group is the divisor of the order of the group.*

Proof : Let H be a sub-group of a finite group G

To prove : $O(H)/O(G)$.

Let $O(H) = m$ and $O(G) = n$.

Since H is a sub-group of G,

$\therefore$ $O(H) \leqslant O(G)$ *i.e.* $m \leqslant n$.

Two cases arise :

Case I. *When* $G = H$.

Here $m = n$

Then the result is obviously true.

[$\because$ *Every element is a divisor of itself*]

Case II. *When* $G \neq H$.

$\therefore$ $\exists$ some $a \in G$ such that $a \notin H$.

Now $O(H) = m$

$\Rightarrow$ H has m different elements.

Let $h_1, h_2, ..., h_m \in H$ ...(I)

All these elements are different.

Consider a new set :

$h_1a, h_2a, ..., h_ma$ ...(II)

All these $\in G$.

[*$a \in G$ and $h_1, h_2, ..., h_m \in G$*
Also H is a sub-group of G
$\therefore$ $h_i \in H \Rightarrow h_i \in G$
$\therefore$ $a \in G, h_i \in G \Rightarrow h_ia \in G$ ($\because$ *G is closed*)]

All the elements of (II) are different :

If possible, let $h_ia = h_ja$

$\Rightarrow$ $h_i = h_j$ [*By Right Cancellation Law*]

which is a contradiction. [$\because$ $h_i \neq h_j$]

Thus all the elements of (II) are different.

Again all the elements of (I) are different from those of (II),

If possible, let $h_ia = h_j$

$\Rightarrow$ $h_i^{-1}h_ia = h_i^{-1}h_j$

[*Pre-multiplying by h_i^{-1}, which $\in G$*
$\because$ $h_i \in H \Rightarrow h_i \in G$]

$\Rightarrow$ $ea = h_i^{-1}h_j$

$\Rightarrow$ $a = h_i^{-1}h_j$

Now $h_i \in H, h_j \in H$

$\Rightarrow$ $h_i^{-1} \in H, h_j \in H$

$\Rightarrow$ $h_i^{-1} h_j \in H$ [$\because$ *H is closed*]

$\therefore$ $a = h_i^{-1} h_j \in H \Rightarrow a \in H$,

which is contradiction. [$\because$ $a \notin H$]

Thus all the elements of (I) are different from the elements of (II).

$\therefore$ O(H)$=m$, O(G)$=2m$, and $m/2m$

Thus O(H)/O(G).

If G is not exhausted, let some $b \in G$ such that b is neither in list (I) nor in list (II).

Consider a new list

$$h_1 b, \; h_2 b, \ldots\ldots\ldots h_m b \qquad \ldots\text{(III)}$$

All these $\in G$

[$\because$ $h_i \in H \Rightarrow h_i \in G$ *and* $b \in G \Rightarrow h_i b \in G$ ($\because$ *G is closed*)]

The elements of (III) are different.

If possible, let $h_i b = h_j b$

$\Rightarrow$ $h_i = h_j$, [*By right cancellation law*]

which is a contradiction [$\because$ $h_i \neq h_j$]

Thus all the elements of (III) are different.

The elements of (III) are different from those of (I) :

If possible, let $h_i b = h_j$

$\Rightarrow$ $h_i^{-1} h_i b = h_i^{-1} h_j$

[*Pre-multiplying by* h_i^{-1}, *which* $\in G$ $\therefore$ $h_i \in H \Rightarrow h_i \in G$]

$\Rightarrow$ $eb = h_i^{-1} h_j$

$\Rightarrow$ $b = h_i^{-1} h_j$

Now $h_i \in H, h_j \in H$

$\Rightarrow$ $h_i^{-1} \in H, h_j \in H$

$\Rightarrow$ $h_i^{-1} h_j \in H$ [$\because$ *H is closed*]

$\therefore$ $b = h_i^{-1} h_j \in H \Rightarrow h \in H$,

which is a contradiction. [$\because$ $b \notin H$]

Thus all the elements of (III) are different from the elements of (I).

The elements of (III) are different from those of (II) :

If possible, let $h_i b = h_j a$

$\Rightarrow$ $h_i^{-1} h_i b = h_i^{-1} h_j a$][*Pre-multiplying by* h_i^{-1}, *which* $\in G$ $\therefore$ $h_i \in H \Rightarrow h_i \in G$]

$\Rightarrow$ $eb = h_i^{-1} h_j a$

$\Rightarrow$ $b = h_i^{-1} h_j a$

$\Rightarrow$ $b \in$ list (II),

which is a contradiction.

Thus all the elements of (III) are different from those of (II).

Now if G is exhausted, then $O(G)=3m$

and $\qquad m \mid 3m \quad \Rightarrow \quad O(H)/O(G)$.

If G is not exhausted, let the process terminate after k (finite) no. of steps.

Then $\qquad O(G)=km \quad$ *i.e.* $\quad n=km$

$\Rightarrow \qquad m/n \qquad\qquad [\because \; m/km]$

$\Rightarrow \qquad O(H)/O(G)$

Hence the theorem.

Converse. The converse of Lagrange's Theorem **does not always hold**, *i.e.* if m is a divisor of n, it is not necessary that G must have a sub-group of order m.

Cor. 1. *The order of every element of a finite group is a divisor of the order of the group.*

Proof : Let G be a finite group.

$\forall \; a \in G$, $O(a)$ must exist

[$\because$ *In a finite group order of every element exists*]

Further let $O(a)=m$.

To prove : $m/O(G) \quad$ *i.e.* $\quad O(a)/O(G)$

Since $\qquad O(a)=m$,

$\therefore$ by def., $\quad a^m=e$.

Consider the set $H=\{e, a, a^2, \ldots\ldots\ldots, a^{m-1}\}$

This must turn out to be *a* sub-group of G.

H is finite $\qquad$ [$\because$ *G is finite*]

To prove : *H is closed.*

$\forall \; a^i, a^j \in H$, where $0 \leqslant i, j < m$

$$\begin{aligned} a^i \cdot a^j &= a^{i+j} \\ &= a^{mq+r} \qquad [\because \; i+j=mq+r, \text{ where } 0 \leqslant r < m] \\ &= a^{mq} \cdot a^r \\ &= (a^m)^q \cdot a^r \\ &= e^q \cdot a^r \\ &= e \cdot a^r \\ &= a^r \in H \qquad [\because \; 0 \leqslant r < m] \end{aligned}$$

Thus H is a sub-group [$\because$ *H is finite, then only condition of sub-group is :* $\forall \, a, b \in H \Rightarrow ab \in H$]

Also $\qquad O(H)=m$.

To prove : All the elements of H are different.

If possible, let $\quad a^i=a^j$, where $j>i$

$\Rightarrow \qquad a^i \cdot a^{-i}=a^j \cdot a^{-i} \qquad$ [*Post-multiplying by* a^{-i}]

$\Rightarrow \quad a^0 = a^{j-i}$

$\Rightarrow \quad e = a^{j-i} \quad \Rightarrow \quad a^{j-i} = e$

Bu $\quad O(a) = m$

$\Rightarrow \quad m \mid (j-i). \qquad [\because \; j, i < m \text{ and } j > i$

$\Rightarrow \; j-i > 0 \text{ and } j-i < m]$

which is not true. $\qquad$ [$\because$ *m can't divide a number which is* $<m$]

Thus all the elements of H are different.

$\therefore \quad O(H) = m$

But $\quad O(H)/O(G) \qquad$ [*Lagrange's Theorem*]

$\Rightarrow \quad m/O(G)$

Hence $\quad O(a)/O(G).$

Cor. 2. *If G be a finite group, then for all* $a \in G$, $a^{O(G)} = e$.

Proof: Let $\quad O(G) = n$

$\forall \; a \in G, \quad O(a)$ must exist $\qquad$ [$\because$ *G is finite*]

Further let $\quad O(a) = m$

Then by def., $\quad a^m = e$

Since $\quad O(a)/O(G) \qquad$ [*Cor. 1*]

$\therefore \quad m/n$

$\Rightarrow \quad n = mq$

Now from (1), $\quad a^m = e.$

Raising both sides to the power q, we get

$$(a^m)^q = e^q \quad \Rightarrow \quad a^{mq} = e$$

$\Rightarrow \quad a^n = e$

Hence $\quad a^{O(G)} = e.$

Example 33. *Prove that a group of prime order can't have a proper sub-group.*

Sol. Let $O(G) = p$, where p is a prime number.

Let H be any sub-group of G.

Then $\quad O(H)/O(G) \qquad$ [*By Lagrange's Theorem*]

$\Rightarrow \quad O(H)/p \quad \Rightarrow \quad O(H) = 1$ or p.

Case I. *When* $O(H) = 1$.

Here $\quad H = \{e\}.$

Case II. *When* $O(H) = p$.

Here $\quad O(H) = p = O(G)$

$\Rightarrow \quad G = H.$

Thus H either contains identity alone or $H = G$ itself.

But $H = \{e\}$ or $H = G$ are trivial (*i.e.* improper) sub-groups of G.

Hence G can't have a proper sub-group.

CYCLIC GROUPS

Def. *A group G is said to be cyclic if there exists an element $a \in G$, such that every element of G is a power of a.*

Here a is called the **generator** and G is denoted by $<a>$.

If the composition in G is denoted **additively** then *G is a cyclic group if there exists an element a of G such that every element of G is of the form na, where n is an integer.*

Infinite Cyclic and Finite Cyclic Groups.

Let G be a cyclic group.

$\therefore\ \exists\, a \in G$ s.t $G = <a>$.

Then $G=\{\ldots\ldots a^{-2}, a^{-1}, e, a, a^2, \ldots\ldots\}$.

Now two cases arise :

Case I. *When O (a) does not exist $\forall\ a \in G$.*

To prove : No two powers of a can be equal.

Proof : If possible, let $a^i=a^j$, where i, j are different integers and $i<j$.

Now $\qquad a^i=a^j$

$\Rightarrow \qquad a^i.a^{-j}=a^j.a^{-j}$ [*Post-multiplying by a^{-j}*
$\because\ a^j \in G \Rightarrow a^{-j} \in G$ as G is a group]

$\Rightarrow \qquad a^{i-j}=a^0$

$\Rightarrow \qquad a^{i-j}=e$, where $i-j$ is a +ve integer.

Now there will be many +ve integers of this type and by well ordering principle, the set of positive integers must have the smallest integer. Let m be the smallest +ve integer.

$\therefore \qquad a^m=e \qquad \Rightarrow \quad O(a)=m$

$\Rightarrow$ O(a) exists, which is a contradiction.
[$\because$ *O(a) does not exist*]

Hence all the elements of G are different.

$\therefore\ \forall\ a \in G,\ G=\{\ldots\ldots a^{-2}, a^{-1}, e, a, a^2, \ldots\ldots\}$

$\therefore$ O(G) is not finite [$\because$ *No two powers of a are equal*]

$\therefore$ G is an infinite cyclic group.

Hence if O(a) does not exist, then G is an infinite cyclic group.

Case II. *When O(a) exists.*

Let $O(a)=m$, where m is some finite positive integer.

$\therefore \qquad G=\{e, a, a^2, \ldots\ldots, a^{m-1}\}$.

To prove : No two elements of G are equal.

Proof : If possible, let $a^i=a^j$, where $0 \leq i, j \leq m-1$ and $i<j$

Operating by a^{-j} on both sides, we get :—

$$a^i.a^{-j}=a^j.a^{-j}$$

$$\Rightarrow \quad a^{i-j}=a^0=e.$$

Now $i-j<m$ and $a^{i-j}=e$, which is a contradiction.

[$\because$ We get identity after raising the power]

$\therefore$ All the elements of G are different.

To prove : If we consider any other power of a ; say a^n $\forall n \in I$, then a^n will also belong to the same set.

Proof : Let $n=mq+r$, where $0 \leqslant r<m$.

Now $\quad a^n=a^{mq+r}$

$=a^{mq}.a^r=(a^m)^q.a^r$

$=e^q.a^r \qquad [\because \; a^m=e]$

$=e.a^r \qquad [\because \; e^q=e]$

$=a^r \in G \qquad [\because \; 0 \leqslant r \leqslant m-1]$

Even if n is $-$ve, we get the same result.

$\therefore$ G consists of exactly these elements and nothing more.

$\therefore \quad O(G)=m$ and G is finite.

Hence $\quad O(G)=O(a)$.

Another Form. *If $O(a)$ exists, then $O(a)=O(G)$.*

THEOREMS

Theorem I. *Every cyclic group must be abelian.*

Proof : Let G be a cyclic group such that $G=\langle a \rangle$, where $a \neq e$.

Consider any x, $y \in G$.

$x \in G \quad \Rightarrow \quad x=a^m$, where $m \in I$

[$\because$ *By def. x is some integral power of a*]

$y \in G \quad \Rightarrow \quad y=a^n$, where $n \in I$

[$\because$ *By def. y is some integral power of a*]

Now $\; xy=a^m \,.\, a^n=a^{m+n}$

$=a^{n+m} \qquad [\because \; m, n \in I, \;\therefore\; m+n=n+m]$

$=a^n \,.\, a^m$

$=yx$

Hence G is abelian.

Converse may not hold.

Theorem II. Every sub-group of a cyclic group is cyclic.

Proof : Let G be a cyclic group.

$\therefore \;\exists$ some $a \in G$ such that $G=\langle a \rangle$

Let H be any sub-group of G.

To prove : H is cyclic.

i.e. $\exists$ some element $\in$H such that all the elements of H are generated by that element.

Proof : $\forall\ x \in H \Rightarrow x \in G$ [$\because$ *G is cyclic*]

$\Rightarrow x = a^k$, where $k \in I$.

To prove : H contains some element with +ve power of a.

Proof : (*i*) *If k is a +ve integer,*

then this step is established.

(*ii*) *If k is a −ve integer,*

then $a^k \in H$ [$\because$ *H is a sub-group*]

$\Rightarrow \quad (a^k)^{-1} \in H$ [$\because$ *H is a group in itself*]

$\Rightarrow \quad a^{-k} \in H$ [$\because$ *k is −ve* $\Rightarrow$ *−k is +ve*]

Thus H contains some elements with positive powers of a and out of these, there will be some smallest. Let m be the smallest such that $a^m \in H$.

To prove : a^m works as the generator of H

i.e. $H = \langle a^m \rangle$.

Proof : $\forall\ y \in H \Rightarrow y \in G$ [$\because$ *H is a sub-group of G*]

$\Rightarrow \quad y = a^n$, where $n \in I$

$n = mq + r$, where $0 \leqslant r < m$.

Now $a^m \in H \Rightarrow (a^m)^q \in H$

$\Rightarrow \quad a^{mq} \in H$

$\Rightarrow \quad (a^{mq})^{-1} \in H$ [$\because$ *H is a group in itself*]

$\Rightarrow \quad a^{-mq} \in H$

Now $a^n \in H, a^{-mq} \in H \Rightarrow a^n \cdot a^{-mq} \in H$ [$\because$ *H is closed*]

$\Rightarrow \quad a^{n-mq} \in H$

$\Rightarrow \quad a^r \in H$

But $r < m$ and m is the smallest +ve integer such that $a^m \in H$.

$\therefore \quad r = 0$ is the only possibility

$\therefore \quad n = mq$.

Now $a^n = a^{mq} = (a^m)^q$.

$\therefore$ Any element of H can be obtained from the element a^m.

Hence H is cyclic and a^m works as the generator.

Remember : Identity can't be the generator of any group, in general, except in a special group where there is only one element *viz.* identity.

Theorom III. Every group of prime order is cyclic.

Proof : Let O(G) $= p$, where p is a prime number.

Let $a (\neq e) \in G$.

Consider a sub-group generated by a.

Let $H=<a>$

$\Rightarrow \quad O(H)>1$

$[\because \; H=<a> \Rightarrow a \in H \text{ and also } e \in H \Rightarrow O(H)>1]$

Since H is a sub-group of G, then by Lagrange's Theorem,

$O(H)/O(G) \Rightarrow O(H)/p$

$\Rightarrow \; O(H)=1 \text{ or } p$ $\qquad [\because \; p \text{ is prime}]$

But $O(H)>1$, $\quad \therefore \; O(H)\neq 1$.

Thus $\; O(H)=p=O(G)$

$\therefore \qquad G=H.$

But H is a cyclie group, $\therefore$ G is also cyclic group.

Hence the result.

Example 34. *Which of the following groups are cyclic ?*

(*i*) $G=<Z, +>$

(*ii*) $G=<Q, +>$

(*iii*) $G=\{6^n/n \in Z\}$.

Sol. (*i*) G is cyclic. Here 1 and -1 are its generators

(*ii*) $G=\left\{\frac{p}{q}, q\neq 0, +\right\}$ is not cyclc.

(*iii*) G is cyclic. Here 6 and $\frac{1}{6}$ are its generators.

Example 35. *Prove that the additive group G of all integers is cyclic.*

Sol. Clearly $1 \in Z$.

All the elements of this group are obtainable by 1.

Since the operation is '+',

$\therefore \; 1^2=1+1=2$

$1^3=1+1+1=3$

$1^0=0$

$1^{-1}=\text{Inverse of } 1=-1$

$1^{-2}=(1^2)^{-1}=(1+1)^{-1}=2^{-1}=-2$; and so on.

$\therefore$ This group is cyclic and 1 is the generator.

Also inverse of 1 *i.e.* -1 is the generator.

i.e. if $G=<1>$, then $G=<-1>$.

To prove : *There are no more generators.*

Proof : Consider 2.

Now 2 can't be the generator ; $\quad [\because$ *1 is not obtainable by 2*] and so on.

Hence there are **exactly** two generators.

Example 36. *Prove that every group of composite order must possess proper sub-groups.*

Sol. Let G be a group so that $O(G)=n$, where n is a finite composite number.

Two cases arise :

Case I. *When G is cyclic.*

Then corresponding to every divisor of the order of the group, there exists a sub-group of that order which will be a proper sub-group.

Case II. *Where G is not cyclic.*

Here there exists no element of G from which we can obtain all the elements of G.

Let $\quad a(\neq e)\in G.$

Consider a sub-group generated by a.

Let $\quad H=<a>.$

Then H will be proper sub-grou pof G.

[$\because$ *All the elements of G can't be obtained from a*]

Example 37. *Prove that every group of prime order must be abelian.* **(Imp.)**

Sol. [*Here we shall show that a group of prime order is cyclic and then every cyclic group is abelian.*]

Let $\quad O(G)=p$, where p is a prime number.

Let $\quad a(\neq e)\in G.$

Consider $\quad H=<a>$, a sub-group generated by a.

Clearly $O(H)>1$.

Now $O(H) \mid O(G)$ [*By Lagrange's Theorem*]

$\Rightarrow \quad O(H) \mid p$

$\Rightarrow \quad O(H)=1$ or p [$\because$ *p is prime*]

But $\quad O(H)\neq 1$ [$\because$ *$O(H)>1$*]

$\Rightarrow \quad O(H)=p=O(G)$

$\Rightarrow \quad G=H.$

But H is cyclic

G is cyclic.

To prove : *Every cyclic group must be abelian.*

Since G is cyclic [*Proved above*]

$\therefore \quad \exists\ (a\neq e)\in G$ s.t. $=G<a>.$

Now $\forall\ x.\ y\in G$

$\Rightarrow \quad x=a^n$, where $n\in Z$ [$\because$ *G is cyclic,*

and $\quad y=a^m$, where $m\in Z$ $\quad\therefore$ *each element of G is some power of a*]

Now $\quad xy=a^n \cdot a^m$

$\quad\quad =a^{n+m}=a^{m+n} \quad [\because \quad m, n\in Z \Rightarrow m+n=n+m]$

$\quad\quad =a^m \cdot a^n=yx$

Thus G is abelian.

Hence the result.

(*i*) **Complex.** **Def.** *Let G be a group. Then the complex of a group G means the sub-set of G which may not be a sub-group.*

(*ii*) **Multiplication of two complexes.** Let A and B be two complexes of a group G, *i.e.*

$$A\subset G \quad \text{and} \quad B\subset G.$$

Then $\quad AB=\{ab \mid a\in A, b\in B\}$

Since $A\subset G$, $\quad \therefore$ if $a\in A$, then $a\in G$.

Since $B\subset G$, $\quad \therefore$ if $b\in B$, then $b\in G$.

Now $a, b\in G \quad \Rightarrow \quad ab\in G \quad [\because \quad$ *G is closed*]

Also $\quad BA=\{ba \mid b\in B, a\in A\}$

Now $AB\subset G$ and $O(AB)=O(A)\, O(B)$.

In general, $\quad AB\neq BA$ | **C.T.M.**

but $\quad AB=BA$ if the group is abelian.

(*iii*) Let H and K be sub-groups of a group G.

Then $\quad HK=\{hk \mid h\in H, k\in K\}$

Since $H\subset G$, $\quad \therefore$ if $h\in H$, then $h\in G$.

Since $K\subset G$, $\quad \therefore$ if $k\in K$, then $k\in G$.

Now $h, k\in G \quad \Rightarrow \quad hk=G \quad [\because \quad$ *G is closed*]

$\therefore \quad HK\subset G$.

Theorem I. *Prove that HK is a sub-group of G iff HK=KH.* [G.N.D.U. 1977] **(V. Imp.)**

Given : $HK=KH$.

To prove : HK is a sub-group of G.

i.e. we have to establish that

(*i*) $\forall\ x, y\in HK \quad \Rightarrow \quad xy\in HK$ (*Closure*)

(*ii*) $\forall \quad x\in HK \quad \Rightarrow \quad x^{-1}\in HK.$ (*Inverse*)

Proof : (*i*) Let $x=hk\in HK$ and $y=h'k'\in HK$.

Then $\quad xy=hk\, h'k'$.

But since $kh'\in KH=HK \quad [\because \quad HK=KH]$

$\therefore \quad kh'=h_2k_2$ with $h_2\in H$, $k_2\in H$

$\therefore \quad xy=h(h_2k_2)k'=(hh_2)(k_2k')\in HK.$

Thus *HK is closed.*

(*ii*) $x^{-1}=(hk)^{-1}$

$=k^{-1}h^{-1}$

$\in KH$ $[\because h\in H \Rightarrow h^{-1}\in H, k\in K \Rightarrow k^{-1}\in K]$

$\in HK$ $[\because HK=KH]$

Thus inverse of every element of HK exists.

Hence HK is a sub-group.

Converse. Given : HK is a sub-group of G.

To prove : HK=KH

i.e. we have to est blish that

(*i*) $HK\subseteq KH$

(*ii*) $KH\subseteq HK$.

Proof : (*i*) Since HK is a sub-group of G,

$\therefore \quad \forall h\in H, k\in K, \; h^{-1}k^{-1}\in HK$

$\Rightarrow \quad (h^{-1}k^{-1})^{-1}\in HK$ $[\because$ *HK is a sub-group*$]$

$\Rightarrow \quad (k^{-1})^{-1}(h^{-1})^{-1}\in HK$

$\Rightarrow \quad kh\in HK.$

But kh is any element of KH.

$\therefore \quad KH\subseteq HK$ ...(1)

(*ii*) Let $x\in HK \Rightarrow x^{-1}\in HK$ $[\because$ *HK is a sub-group*$]$

$\Rightarrow x^{-1}=hk$

and so $x=(x^{-1})^{-1}=(hk)^{-1}=k^{-1}h^{-1}\in KH.$

Thus $HK\subseteq KH$ ...(2)

Combining (1) and (2), HK=KH.

Cor. *If H, K are sub-groups of abelian group G, then HK is a sub-group of G.*

Since G is abelian. $\therefore$ trivially HK=KH.

By the above theorem, HK is a sub-group of G.

Theorem II. *If H and K are finite sub-groups of G of orders O(H) and O(K) respectively, prove that*

$$O(HK)=\frac{O(H)\,.\,O(K)}{O(H\cap K)}.$$ [G.N.D.U. 1976] **(V. Imp.)**

Two cases arise :

Case I. *When* $O(H\cap K)=1$.

To prove : $O(HK)=O(H)\times O(K)$.

Proof : Since $O(H \cap K)=1$

$\therefore$ In the list of all elements of HK, there is no repetition of elements.

If we list all the elements hk, $h \in H$, $k \in K$, then some element in the list may appear twice. *i.e.*, for some $h \in H$ $(h \neq h_1)$, $hk = h_1 k_1$

$\Rightarrow \quad h_1^{-1}(hk)=h_1^{-1}(h_1k_1)$ [*Pre-multiplying by* h_1^{-1}]

$\Rightarrow \quad h_1^{-1}(hk)k^{-1}=h_1^{-1}(h_1k_1)k^{-1}$ (*Post-multiplying by* k^{-1}]

$\Rightarrow \quad h_1^{-1}h(kk^{-1})=(h_1^{-1}h_1)k_1k^{-1}$

$\Rightarrow \quad h_1^{-1}he \quad =ek_1k^{-1}$

$\Rightarrow \quad h_1^{-1}h \quad =k_1k^{-1}$

Since $h_1 \in H$, $h_1^{-1} \in H$ [$\because$ *H is a sub-group*]

Thus $\quad h_1^{-1}h \in H$ [$\because$ *H is closed*]

Similarly $\quad k_1k^{-1} \in K$.

Both $\quad h_1^{-1}h$ and $k_1k^{-1} \in H \cap K$

But $\quad O(H \cap K)=1$ [*Given*]

$\therefore \quad H \cap K=\{e\}$

$\therefore \quad h_1^{-1}h=e$

$\Rightarrow \quad h_1h_1^{-1}h=h_1e$ [*Pre-multiplying by* h_1]

$\Rightarrow \quad eh=h_1e$

$\Rightarrow \quad h=h_1$.

which is a contradiction. [$\because$ *We have assumed that* $h \neq h_1$]

Thus if $O(H \cap K)=1$, then there is no repetition in the elements of HK.

Hence $O(HK)=O(H).O(K)$.

Case II. *When* $O(H \cap K)>1$.

To prove : *In the list of elements of HK, every element is repeated exactly* $O(H \cap K)$ *times.*

Proof : Let $x \in (H \cap K)$ *i.e.*, $x \in H$, $x \in K$.

Consider $hk \in HK$, where $h \in H$, $k \in K$.

Now $\quad hk=hek$ | **Note it**

$\quad =hxx^{-1}k$ [$\because$ $xx^{-1}=e$]

$\quad =(hx)(x^{-1}k)$

Now $\quad hx \in H$ [$\because$ $h \in H$, $x \in H \Rightarrow hx \in H$ *as H is closed*]

and $\quad x^{-1}k \in H$ [$\because$ $x \in K \Rightarrow x^{-1} \in K$ as *K is a sub-group*

$\therefore$ $x^{-1} \in K, k \in K \Rightarrow x^{-1}k \in K$ *as K is closed*]

Thus each element of HK is **repeated at least** $\mathbf{O(H \cap K)}$ **times.**

To prove : *Each element is repeated exactly $O(H\cap K)$ times.*

Proof : Let $hk=h_1k_1$ ...(1),

where $h, h_1 \in H$ and $k, k_1 \in K$

$\Rightarrow \quad h^{-1}hk=h^{-1}h_1k_1$ [*Pre-multiplying by h^{-1}*]

$\Rightarrow \quad ek=h^{-1}h_1k_1$

$\Rightarrow \quad k=h^{-1}h_1k_1$

$\Rightarrow \quad kk_1^{-1}=h^{-1}h_1k_1k_1^{-1}$ [*Post-multiplying by k_1^{-1}*]

$\Rightarrow \quad kk_1^{-1}=h^{-1}h_1e$

$\Rightarrow \quad kk_1^{-1}=h^{-1}h_1$

Now $kk_1^{-1}\in H$ $\quad\therefore\quad h^{-1}h_1\in K$

Also $\quad h^{-1}h_1\in H.$

Let $\quad h^{-1}h_1=u=kk_1^{-1}$

$\therefore \quad u\in H\cap K$

Now $\quad h^{-1}h_1=u$

$\Rightarrow \quad hh^{-1}h_1=hu$ [*Pre-multiplying by h*]

$\Rightarrow \quad eh_1=hu$

$\Rightarrow \quad h_1=hu$ ...(2)

Also $\quad kk_1^{-1}=u$

$\Rightarrow \quad k^{-1}kk_1^{-1}=k^{-1}u$ [*Pre-multiplying by k^{-1}*]

$\Rightarrow \quad ek_1^{-1}=k^{-1}u$

$\Rightarrow \quad k_1^{-1}=k^{-1}u$

$\Rightarrow \quad (k_1^{-1})^{-1}=(k^{-1}u)^{-1}$ [*Taking inverses*]

$\Rightarrow \quad k_1=u^{-1}k$ ...(3)

Now from (1), $hk=h_1k_1$

$\qquad =(hu)(u^{-1}k),$ [*Using (2) and (3)*]

which is of the same type $(hx)(x^{-1}k)$.

It follows that there are no more repetitions.

Thus each element of HK is repeated exactly $O(H\cap K)$ times.

Hence $\quad O(HK)=\dfrac{O(H).O(K)}{O(H\cap K)}$.

Cor. 1. *If H and K are sub-groups of G and given that $O(H)>\sqrt{O(G)}$ and $O(K)>\sqrt{O(G)}$, prove that $O(H\cap K)>1$.*

Proof : We know that $HK=\{hk \mid h\in H, k\in K\}$.

Now $h\in H \Rightarrow h\in G$ [$\because$ *H is a sub-group of G*]

and $\quad k\in K \Rightarrow k\in G$ [$\because$ *K is a sub-group of G*]

$\therefore\quad h\in G, k\in G \quad\Rightarrow\quad hk\in G$ [$\because$ *G is closed*]

Hence $HK \subset G$

$\therefore \quad O(HK) \leqslant O(G)$

$$\Rightarrow \quad O(G) \geqslant O(HK) = \frac{O(H).O(K)}{O(H \cap K)} \quad \ldots(1)$$

Now $\dfrac{O(H).O(K)}{O(H \cap K)} > \dfrac{\sqrt{O(G)} \cdot \sqrt{O(G)}}{O(H \cap K)}$

i.e., $\dfrac{O(H).O(K)}{O(H \cap K)} > \dfrac{O(G)}{O(H \cap K)}$

From (1), $\quad O(G) > \dfrac{O(G)}{O(H \cap K)}$

This is possible only if $O(H \cap K) > 1$.

Cor. 2. *If G is a group and $O(G)=pq$, where p and q are prime numbers and $p>q$, prove that it can't contain more than one sub-groups of order p.*

Proof : If possible, let H and K be two sub-groups of order p.

$\therefore \quad O(H)=p$ and $O(K)=p$

Since $p>q$ [*Given*]

$\therefore \quad p^2>pq \quad \Rightarrow \quad p>\sqrt{pq}$.

But $O(H)=O(K)=p$ and $O(G)=pq$

$\therefore \quad O(H)>\sqrt{O(G)}$ and $O(K)=\sqrt{O(G)}$

Then by Cor. 1, $O(H \cap K)>1$ ...(1)

Now $\quad H \cap K$ is a sub-group of H,

$\therefore \quad O(H \cap K)/O(H)$ [*By Lagrange's Theorem*]

$\Rightarrow \quad O(H \cap K)/p$

$\Rightarrow \quad O(H \cap K)=1$ or p [$\because$ *p is a prime number*]

But $\quad O(H \cap K) \neq 1$ [$\because$ *by (1),* $O(H \cap K)>1$]

$\therefore \quad O(H \cap K)=p=O(H)$

$\Rightarrow \quad H \cap K=H$ ...(2)

Similarly $H \cap K=K$ ...(3)

From (2) and (3), $H \cap K=H=K$.

Hence there is only one sub-group of order p.

Theorem III. *If G is a group and H is its sub-group, prove that $HH=H$.* **(Imp.)**

In order to prove $HH=H$, we have to establish that

(*i*) $HH \subseteq H$ and (*ii*) $H \subseteq HH$.

(*i*) **To prove :** $HH \subseteq H$.

Let $x = h_1 h_2 \in HH$, where $h_1 h_2 \in H$.

Now $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$ [$\because$ *H is closed*]

$\Rightarrow \quad x \in H$

But x is arbitrary.

$\therefore \quad HH \subseteq H$ ...(1)

(*ii*) **To prove :** $H \subseteq HH$.

$\forall\, h \in H \Rightarrow he \in HH$ [$\because$ $h, e \in H \Rightarrow he \in HH$]

$\Rightarrow \quad h \in HH$

But h is arbitrary.

$\therefore \quad H \subseteq HH$ ...(2)

From (1) and (2), $H = HH$.

Cor. *Prove that $H^n = H$ ($n \neq 0$), where H is a sub-group of G.*

Proof : $H^1 = H$

and $H^2 = HH = H$ [*Theorem III*]

Let us assume that the result is true for $n = k$.

$\therefore \quad H^k = H$.

Now $H^{k+1} = H^k.H$

$= HH$ [$\because$ *$H^k = H$, assumed above*]

$= H$ [*Theorem III*]

$\therefore$ The result is true for $n = k+1$.

$\therefore$ By Induction Method, $H^n = H$ is true, where n is any positive integer.

To prove : $H = H^{-1}$.

For this we shall establish that

(*i*) $H^{-1} \subseteq H$ and (*ii*) $H \subseteq H^{-1}$.

Proof : (*i*) $\forall\, x \in H^{-1} \Rightarrow x = h^{-1}$

and $\because \quad h \in H \Rightarrow h^{-1} \in H$ [$\because$ *H is a sub-group*]

$\Rightarrow \quad x \in H^{-1}, x \in H$.

But x is arbitrary.

$\therefore \quad H^{-1} \subseteq H$ ...(1)

(*ii*) $\forall\, h \in H \Rightarrow h^{-1} \in H$

Also $H = (h^{-1})^{-1} \in H^{-1} \Rightarrow h \in H^{-1}$

But h is arbitrary.

$\therefore \quad H \subseteq H^{-1}$ ...(2)

From (1) and (2), $H = H^{-1}$.

If $n=-m$, where m is a +ve integer.

Now $\quad H^n=H^{-m}=(H^{-1})^m$

$=H^m \quad$ [$\because$ *$H^{-1}=H$, proved above*]

$=H \quad$ [$\because$ *m is a +ve integer*]

Hence the result $H^n=H$, where n is any integer except zero.

NORMAL SUB-GROUPS

Def. I. *A sub-group H of a group G is said to be normal sub-group of G if for every $g\in G$ and $n\in N$, $g\,n\,g^{-1}\in N$.*

This is also called **invariant sub-group** or **self-conjugate sub-group.**

Notation. The normal sub-group of G is written as $N \lhd G$.

Def. II. *A sub-group N of a group G is said to be normal sub-group of G if for every $g\in G$, $gNg^{-1}\subseteq N$.*

Conclusion. Definitions I and II are equivalent.

Remark. Every group G possesses at least two normal sub-groups viz. G itself and the sub-group containing identity alone. These are called **Improper Normal Sub-groups.**

Simple Group. Def. *A group having no proper normal sub-group is called a simple group.*

Remark. Every group of prime order is simple.

[$\because$ *Such a group has no proper sub-groups (By Lagrange's Theorem)*]

Remark. Let H be a sub-group of G. Let $g\in G$.

Then Hg is called the **right coset ;**

and $\quad gH$ is called the **left coset.**

When the group is abelian, then $gH=Hg$

i.e. $\quad$ left coset=right coset.

When the group is non-abelian, then left coset may or may not be equal to right coset.

i.e. $\quad gH=Hg$

or $\quad gH\neq Hg$.

Special Case. There are special sub-groups which are non-abelian but left coset=right coset.

These are called **Normal Sub-groups.**

THEOREMS

Theorem I. *Every sub-group of an abelian group is a normal sub-group.*

Let H be any sub-group of G.

To prove : H is a normal sub-group,

i.e., $\quad ghg^{-1}\in H \;\; \forall g\in G, \; \forall h\in H$

Proof. $ghg^{-1}=hgg^{-1}$ [$h\in H \Rightarrow h\in G$
$\forall g,\ h\in G \Rightarrow gh=hg$ as G is abelian]

$=he$

$=h\in$ H.

Thus $ghg^{-1}\in$ H.

Hence H is a normal sub-group.

Theorem II. *N is a normal sub-group of G iff $gNg^{-1}=N$ for every $g\in G$.* **(Imp.)** [*G.N.D.U. 1977*]

Let G be a group and N a sub-group of G.

Given. $gNg^{-1}=N\ \forall g\in G$.

To prove. N is a normal sub-group of G.

Proof. $gNg^{-1}=N$ [*Given*]

$\Rightarrow$ $gNg^{-1}\subseteq N$

$\Rightarrow$ N is a normal sub-group of G. [*By def. II*]

Converse :

Given. N is a normal sub-group of G.

To prove. $gNg^{-1}=N\ \forall g\in G$.

Proof. Since N is a normal sub-group of G, [*Given*]

$\therefore$ $gNg^{-1}\subseteq N\ \forall g\in G$ ...(1) [*By def. II*]

Now $g\in G \Rightarrow g^{-1}\in G$ [$\because$ *G is a group*]

Since N is a normal sub-group of G,

$\therefore$ $g^{-1}N(g^{-1})^{-1}\subseteq N$ [*By def.*]

$\Rightarrow$ $g^{-1}Ng\subseteq N$

$\Rightarrow$ $gg^{-1}Ng\subseteq gN$ [*Pre-multiplying by g*]

$\Rightarrow$ $eNg\subseteq gN$

$\Rightarrow$ $Ng\subseteq gN$

$\Rightarrow$ $Ngg^{-1}\subseteq gNg^{-1}$ [*Post-multiplying by g^{-1}*]

$\Rightarrow$ $Ne\subseteq gNg^{-1}$

$\Rightarrow$ $N\subseteq gNg^{-1}$ ...(2)

Combining (1) and (2),

$gNg^{-1}=N$.

Theorem III. *N is a normal sub-group of G iff every left coset of N in G is a right coset of N in G.*

Given. N is a normal sub-group of G.

To prove. $gN=Ng\ \forall g\in G$.

Proof. Since N is a normal sub-group of G,

$\therefore$ $\forall g,\ gNg^{-1}=N$ [*Theorem II*]

$\Rightarrow$ $gNg^{-1}g=Ng$ [*Post-multiplying by g*]

$\Rightarrow \quad gNe = Ng$

$\Rightarrow \quad gN = Ng$

i.e., left coset = right coset.

Converse :

Given. $gN = Ng \ \forall g \in G$

To prove. N is a normal sub-group of G.

Proof. Since $g = ge \in gN$ [$\because e \in N$]

$\therefore$ g must belong to that right coset which is equal to the left coset gN.

However, g is in right coset Ng and two distinct right cosets have no element in common. So this right coset is unique.

In other words, $gN = Ng$

$\Rightarrow \quad gNg^{-1} = Ngg^{-1}$ [*Post-multiplying by* g^{-1}]

$\Rightarrow \quad gNg^{-1} = Ne$

$\Rightarrow \quad gNg^{-1} = N$

Hence N is normal sub-group of G.

Theorem IV. (*i*) *N is a normal sub group of G iff the product of two cosets of N in G is again a right coset of N in G.*

[Pbi. U. 1978]

(*ii*) *N is a normal sub-group of G iff the product of two left cosets of N in G is again a left coset of N in G*

(V. Important)

Sol. (*i*) **Given.** N is a normal sub-group of G.

To prove. Product of two right cosets of N in G is a right coset of N in G.

Proof. Let Na and Nb be two rights cosets of N in G.

Then $Na \cdot Nb = N(aN)b$

$= N(Na)b$ [*Since N is normal,* $\therefore aN = Na$]

$= Nab$, [$\because NN = N$ *as N is normal*]

which is again a right coset.

Converse :

Given. $Na \cdot Nb = Nab$.

To prove. N is a sub-group of G.

Proof $gNg^{-1} = egNg^{-1} \subseteq NgNg^{-1}$

But $NgNg^{-1} = NNgg^{-1}$ [*Given*]

$= NNe = N$

$\therefore \quad g \cdot Ng^{-1} \subseteq NgNg^{-1} = N$

$\Rightarrow \quad gNg^{-1} \subseteq N \quad \forall g \in G$

$\Rightarrow$ Any element gng^{-1} of gNg^{-1} belongs to N.

$\Rightarrow$ N is a normal in G.

(*ii*) Plhase try yourself.

QUOTIENT GROUPS

Theorem V *If G is a group, N a normal sub-group of G, then the set G/N of all right cosets of N in G, together with the binary composition defined by $(Na)(Nb) = Nab$ for $Na, Nb \in G/N$, is a group.* **(V. Important)** [G.N.D.U. 1976 S ; Pbi. U. 1974]

Proof. (*i*) **Non-empty.**

G/N is non-empty because at least N itself is a right coset.

[$\because$ $N = Ne \in G/N$]

(*ii*) **Closure.** Let $Na, Nb \in G/N$ for some $a, b \in G$.

$\therefore$ $NaNb = Nab \in G/N$ [$\because$ *N is a normal in G*]

Thus G/N is closed.

(*iii*) **Associativity.** Let $Na, Nb, Nc \in G/N$ for some $a, b, c \in N$.

$\therefore$ $(NaNb)Nc = (Nab)Nc = N(ab)c$

and $Na(NbNc) = Na(Nbc) = Na(bc)$

But $(ab)c = a(bc)$ [$\because$ *a, b, c* $\in$ *G and G is a group*]

$\therefore$ $(NaNb)Nc = Na(NbNc)$

Thus associative law holds.

(*iv*) **Existence of Identity.**

Let e be the identity of G.

Then $N = Ne \in G/N$

Now $(Na)(N) = (Na)(Ne) = Nae = Na.$

Again $(N)(Na) = (Ne)(Na) = Nea = Na.$

$\therefore$ $(Na)(N) = Na = (N)(Na).$

Thus N is the identity of G/N.

(*v*) **Existence of Inverse.**

Since $(Na)(Na^{-1}) = Naa^{-1} = Ne = N$

and $(Na^{-1})(Na) = Na^{-1}a = Ne = N$

$\therefore$ $(Na)(Na^{-1}) = N = (Na^{-1})(Na)$

$\therefore$ $(Na)^{-1} = Na^{-1} \in G/N$

Thus the inverse of Na is Na^{-1}.

Hence G/N is a group.

Cor. *If G is abelian, then G/N is also abelian.*

Let $Na, Nb \in G/N$ for some $a, b \in N$.

Now $\quad NaNb = Nab$

$= Nba \quad [\because \ ab = ba$ *as G is abelian*$]$

$= NbNa.$

Hence G/N is abelian.

Now we can define quotient group as.

Quotient Group. Def. *Let G be a group and let N be a normal sub-group of G. Then the set G/N of all right cosets of N in G, together with the binary composition defined by $(Na)(Nb) = Nab$ for all $Na, Nb \in G/N$, is a group, and is called* **quotient group** *of G by N.*

This is also called **factor group.**

Lemma. *For a finite group G and for each normal sub-group N of G, $O(G/N) = O(G)/O(N)$.*

Proof. Let t be the number of distinct cosets of N in G.

Then by Lagrange's Theorem, $O(G) = O(N)t$.

Hence $\quad t = \dfrac{O(G)}{O(N)} \quad$ *i.e.*, $O(G/N) = O(G)/O(N)$.

Example 38. *Show that every sub-group of an abelian group is normal.*

Sol. Let G be an abelian group and H a sub-group of G.

Let x be any element of G and h any element of H.

We have : $\quad xhx^{-1} = xx^{-1}h \quad [\because \ h \in H \Rightarrow h \in G.$

Also $x \in G \Rightarrow x^{-1} \in G$

$\therefore \ hx^{-1} = x^{-1}h$ *as G is abelian*$]$

$= eh = h \in H.$

Hence H is normal in G.

Example 39. *If G is abelian, prove that G/N is also abelian.*

Sol. Let Na and $Nb \in G/N$ for some $a, b \in G$.

Since G is abelian, [*Given*]

$\therefore \quad a, b \in G \Rightarrow ab = ba \quad$ ...(1)

Now $\quad Na \,.\, Nb = NNab \quad [\because$ *Left coset=Right coset*$]$

$= Nab$

$[\because$ *N is a sub-group* $\therefore \ NN = N]$

$= Nba \quad$ [*Using* (*1*)]

$= NNba$

$= Nb \,.\, Na.$

Hence G/N is abelian.

Example 40. *If G is a group, N a normal sub-group of G, then the set G/N of all right cosets of N in G, together with the binary composition defined by* $(N+a)+(N+b)=N+(a+b)$ *for* $N+a, N+b\in G/N$ *is a group.*

Sol. (*i*) **Closure.** Let $N+a$, $N+b\in G/N$ for some $a, b\in G$.

$\therefore \quad (N+a)+(N+b)=N+(a+b)\in G/N.$ [$\because$ *N is normal in G*]

Thus G/N is closed.

(*ii*) **Associativity.** Let $N+a$, $N+b$, $N+c\in G/H$ for some $a, b, c\in N$.

$$\therefore \quad (N+a+N+b)+N+c=(N+a+b)+N+c$$
$$=N+(a+b)+c$$

and
$$N+a+(N+b+N+c)=N+a+(N+b+c)$$
$$=N+a+(b+c).$$

But
$$(a+b)+c=a+(b+c)$$
[$\because$ *a, b, c* $\in$ *G and G is a group*]

$$\therefore \quad (N+a+N+b)+N+c=N+a+(N+b+N+c)$$

Thus associative law holds.

(*iii*) **Existence of Identity.**

Let e be the identity of G.

Then $\quad N=Ne\in G/N.$

Now $\quad (N+a)+(N)=(N+a)+(N+e)$
$$=N+a+e=N+a.$$

Again $\quad (N)+(N+a)=(N+e)+(N+a)$
$$=N+e+a=N+a.$$

$$\therefore \quad (N+a)+N=N+a=N+(N+a).$$

Thus N is the identity of G/N.

(*iv*) **Existence of Inverse.**

Since $(N+a)+[N+(-a)]=N+a+(-a)$
$$=N+e=N.$$

and
$$(N+(-a))+(N+a)=N+(-a)+a$$
$$=N+e=N$$

$$\therefore \quad (N+a)+[N+(-a)]=N=[N+(-a)]+(N+a)$$

$$\therefore \quad (N+a)^{-1}=N+(-a)\in G/N$$

Thus the inverse of $N+a$ *is* $N+(-a)$.

Hence G/H is a group.

Example 41. *If G is a group and H is a sub-group of index 2 in G, prove that H is normal sub-group of G.* **(Important)**

[G.N.D.U. 1976 S]

[**Remember :** *Index of H in G=2 means that there are only two left or two right cosets*]

Let H be a sub-group of index 2 in G.

$\therefore$ The number of distinct right cosets of H in G is 2.

Let x be any element of G.

Two cases arise :

Case I. *When* $x \in H$.

$$x \in H \Rightarrow Hx = H \qquad [\because Hh = H \text{ when } h \in H]$$

Also $\quad x \in H \Rightarrow xH = H$

$\therefore \quad Hx = H = xH$

$\Rightarrow$ H is normal in G

Case II. *When* $x \notin H$.

$$x \notin H \Rightarrow xH \neq H$$

Also $\quad x \notin H \Rightarrow Hx \neq H$

Since H is of index 2, the cosets H, xH and Hx are such that

$$G = H \cup Hx = H \cup xH \qquad ...(i)$$

and

$$\phi = H \cap Hx = H \cap xH \qquad ...(ii)$$

[$\because$ *Each element of G is in some coset and two cosets are disjoint*]

From (*i*) and (*ii*), $\quad xH = Hx \ \forall x \in G$.

Hence H is normal sub-group of G.

Example 42. *If N is a normal sub-group of G and H is any sub-group of G, prove that NH is a sub-group of G.*

(**V. Important**) [G.N.D.U. 1976]

Sol. Since N is a normal sub-group of G, [*Given*]

$\therefore \quad Ng = gN \ \forall g \in G$

Also $\quad \forall h \in H \Rightarrow h \in G \qquad [\because$ *H is a sub-group of G*]

$\therefore \quad Nh = hN \ \forall h \in H$

$\therefore \quad NH = HN$.

Thus N and H are two sub-groups such that NH=HN.

To prove. *NH is a sub-group of G.*

For this we have to prove that

$$(NH)(NH)^{-1} = NH \qquad [\because H \text{ is a sub-group} \Rightarrow HH^{-1} = H]$$

Proof. $(NH)(NH)^{-1} = NH(H^{-1}N^{-1}) = N(HH^{-1})N^{-1}$

$= NH\,N^{-1}$

[$\because$ $HH^{-1} = H$ *as H is a sub-group*]

$= (HN)N^{-1} \qquad [\because NH = HN]$

$= H(NN^{-1})$

$= HN$

$= NH \qquad [\because NH = HN]$

Hence NH is a sub-group of G.

Example 43. *Suppose that N and M are two normal sub-groups of G and that $N \cap M = \{e\}$. Show that for any $n \in N$, $m \in M$, $nm = mn$.* **(V. Important)** [G.N.D.U. 1977]

Sol. Let n be any element of N and m be any element of M. *Consider* $nm\,n^{-1}m^{-1}$.

Since N is normal, $\therefore$ $mn^{-1}m^{-1} \in N$

Also $n \in N$

$\therefore$ $nmn^{-1}m^{-1} \in N$ ...(1)

Again since M is normal, $\therefore$ $nmn^{-1} \in M$

Also $m^{-1} \in M$

$\therefore$ $nmn^{-1}m^{-1} \in M$ ...(2)

From (1) and (2), $nm\,n^{-1}m^{-1} \in N \cap M = \{e\}$

$\Rightarrow$ $nm\,n^{-1}m^{-1} = e$

$\Rightarrow$ $nm\,n^{-1}m^{-1}m = em$ [*Post-multiplying by m*]

$\Rightarrow$ $nmn^{-1}e = em$

$\Rightarrow$ $nm\,n^{-1} = m$

$\Rightarrow$ $nm\,n^{-1}n = mn$ [*Post-multiplying by n*]

$\Rightarrow$ $nme = mn$

$\Rightarrow$ $nm = mn$, which is true.

Example 44. *Let G be a group, H a sub-group of G. Let for $g \in G$, $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$. Prove that gHg^{-1} is a sub-group of G.*

Sol. Let gh_1g^{-1}, gh_2g^{-1} be any two elements of gHg^{-1} where $h_1, h_2 \in H$

Now
$$\begin{aligned}(gh_1g^{-1})(gh_2g^{-1})^{-1} &= gh_1\,g^{-1}(g^{-1})^{-1}\,h_2^{-1}\,g^{-1}\\ &= gh_1\,g^{-1}\,gh_2^{-1}\,g^{-1}\\ &= gh_1\,eh_2^{-1}\,g^{-1}\\ &= gh_1\,h_2^{-1}g^{-1} \in gHg^{-1}\end{aligned}$$

[$\because$ $h_1h_2^{-1} \in H$]

$\therefore$ gHg^{-1} is a sub-group of G.

[$\because$ *If $a, b \in H \Rightarrow ab^{-1} \in H$, then H is a sub-group of G*]

Example 45. *Suppose H is the only sub-group of finite order m in the group G. Prove that H is a normal sub-group of G.*

Sol. Here H is a sub-group of G and $O(H) = m$.

If $x \in G$, then xHx^{-1} is a sub-group of G. [*Ex. 44*]

To prove. $O(xHx^{-1}) = m$.

Proof. Let $H = \{h_1, h_2, \ldots\ldots\ldots, h_m\}$.

Then $xHx^{-1} = \{xh_1x^{-1}, xh_2x^{-1}, \ldots\ldots\ldots, xh_mx^{-1}\}$.

The number of distinct elements in xHx^{-1} is m

$[\because \; xh_i x^{-1}=xh_j x^{-1} \;\Rightarrow\; h_i=h_j]$

$\therefore \qquad O(xHx^{-1})=O(N)=m.$

But H is the only sub-group of G of order m [*Given*]

$\therefore$ we must have $xHx^{-1}=H \;\forall x\in G.$

Hence H is the normal sub-group of G.

Example 46. *If N and M are normal sub-groups of G, prove that NM is also a normal sub-group of G.*

Sol. Since N and M are two normal sub-groups of G,

then $\qquad NM=MN.$

Thus N and M are two normal sub-groups of G such that

$$NM=MN$$

$\Rightarrow \qquad$ NM is a sub-group of G. [*Ex.* 42]

To prove. *NM is a normal sub-group of G.*

Let x be any element of G and nm be any element of NM.

Then for $n\in N$, $m\in M$, we have ;

$x(nm)x^{-1}=xnem\,x^{-1} \qquad [\because\; n\in N \;\Rightarrow\; n\in G$

$\Rightarrow \qquad ne=e$ *as N is a normal sub-group of G*]

$=xn\,x^{-1}xm\,x^{-1} \qquad [\because\; xx^{-1}=e \text{ i.e. } x^{-1}x=e]$

$=(xnx^{-1})(xmx^{-1}) \in NM$

[$\because$ *N is a normal sub-group* $\Rightarrow xnx^{-1}\in N$

and M is normal sub-group $\Rightarrow xmx^{-1}\in M$]

Hence NM is a normal sub-group of G.

Example 47. *If H is a sub-group of G and N is a normal sub-group of G, show that $H\cap H$ is a normal sub-group of H.*

(V. Important)

Sol. Since H and N are sub-groups of G,

$\therefore \qquad H\cap H$ is also a sub-group of G.

Also since $\qquad H\cap N \subseteq H,$

$\therefore \qquad H\cap N$ is a sub-group of H.

To prove. *$H\cap N$ is a normal sub-group of H.*

Let x be any element of H and a be any element of $H\cap N$

$\Rightarrow \qquad a\in H$ and $a\in N$

Since N is a normal sub-group of G,

$\therefore \qquad xa\,x^{-1}\in N \qquad$ ...(1) [*By def.*]

Since H is a sub-group of G,

$\therefore \qquad x\in H,\; a\in H \;\Rightarrow\; xax^{-1}\in H \qquad$ ...(2

From (1) and (2), $xax^{-1} \in H \cap N$

Thus $x \in H, a \in H \cap H \Rightarrow xax^{-1} \in H \cap N$

$\Rightarrow$ $H \cap N$ is a normal sub-group of H.

Example 48. *If H is a sub-group of G and let $N(H) = \{g \in G \mid gHg^{-1} = H\}$, show that*

(i) N(H) is a sub-group of G

(ii) H is a normal sub-group of N(H)

(iii) N(H) is the largest sub-group of G in which H is normal

(iv) H is a normal in G if and only if N(H) = G.

(V. Important)

Sol. *(i)* Let $a, b \in N(H)$.

$\therefore$ $aHa^{-1} = H$ and $bHb^{-1} = H$ [*By def. of N(H)*]

Now $bHb^{-1} = H \Rightarrow b^{-1}(bHb^{-1}) = b^{-1}H$

[*Operating on the left by b^{-1}*]

$\Rightarrow bb^{-1}Hb^{-1} = b^{-1}H$

$\Rightarrow eHb^{-1} = b^{-1}H$

$\Rightarrow Hb^{-1} = b^{-1}H$

$\Rightarrow Hb^{-1}b = b^{-1}Hb$

[*Operating on the right by b*]

$\Rightarrow He = b^{-1}Hb$

$\Rightarrow H = b^{-1}Hb.$

We have : $(ab^{-1})H(ab^{-1})^{-1} = ab^{-1}Hba^{-1}$

$[\because (ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}]$

$= aHa^{-1}$ $[\because H = b^{-1}Hb]$

$= H$ $[\because H = a^{-1}Ha = aHa^{-1}]$

$\therefore$ $ab^{-1} \in N(H)$

Thus $a, b \in N(H) \Rightarrow ab^{-1} \in N(H)$.

Hence N(H) is a sub-group of G.

(ii) Let h be any element of H.

Since $hHh^{-1} = H$, $\therefore$ $h \in N(H)$.

Thus $H \subseteq N(H)$ *i.e.* H is a sub-group of N(H).

To prove. *H is normal in N(H)*

Let x be any element of N(H)

$\therefore$ $xHx^{-1} = H$ [*Def. of N(H)*]

Hence H is a normal sub-group of N(H).

(iii) Let K be any sub-group of G in which H is normal.

To prove. $K \subset N(H)$.

Since H is normal in K,

$\therefore$ $kH = Hk$, where k is any element of K

$\Rightarrow$ $k \in N(H)$

$\Rightarrow$ $K \subset N(H)$

Hence N(H) is the largest sub-group of which H is normal.

(*iv*) Let H be normal in G.

Let $x \in G$. Then $xHx^{-1} = H$ [$\because$ *H is normal in G*].

$\Rightarrow$ $x \in N(H)$

Thus $x \in G \Rightarrow x \in N(H)$.

$\therefore$ $G \subseteq N(H)$

But $N(H) \subseteq G$

Hence $G = N(H)$

Converse. Let $N(H) = G$.

Then $x \in G \Rightarrow x \in N(H)$

$\Rightarrow xHx^{-1} = H$

$\Rightarrow$ H is normal sub-group of G.

HOMOMORPHISM

By '*homo*', we mean '*similar*' and by '*morphism*', we mean '*structure*'.

Thus two groups are **homomorphic** *if they have the similar structure.*

(*a*) **Definition.** *A mapping φ from a group G into a group $\bar{G}$ is said to be homomorphism if* $\forall\ a, b \in G,\ \varphi(a \,.\, b) = \varphi(a) {*} \varphi(b)$.

☞ **We must note that**

(*i*) On R.H.S. in $\varphi(a.b)$, the product $a.b$ is computed in G using the product of elements of G ; and

(*ii*) On L.H.S. in $\varphi(a) {*} \varphi(b)$, using the product of elements of $\bar{G}$.

(*b*) **Isomorphism.** *Let* $\varphi : G \to \bar{G}$ *such that* $\varphi(a.b) = \varphi(a) {*} \varphi(b)$. *If φ is one-one mapping, then it is called isomorphism.*

Thus the groups G and $\bar{G}$ are isomorphic and is denoted as $G \cong \bar{G}$.

(*c*) **Endomorphism.** *Let* $\varphi : G \to G$ *such that* $\varphi(a.b) = \varphi(a) {*} \varphi(b)$. *If φ is a mapping from one group to the same group, then it is called endomorphism.*

From (1) and (2), $\varphi(x)\ \varphi(x^{-1})=\bar{e}$

$\Rightarrow \qquad [\varphi(x)]^{-1}=\varphi(x^{-1}).$

(*iii*) We shall prove this result by Induction Method.

$$\varphi(x^1)=\varphi(x)=[\varphi(x)]^1.$$

Thus the result is true for $n=1$.

Let us assume that the result is true for $n=k$.

$\therefore \qquad \varphi(x^k)=[\varphi(x)]^k.$

Now $\qquad \varphi(x^{k+1})=\varphi(x^k \cdot x)$

$=\varphi(x^k) \cdot \varphi(x)$ [$\because$ *φ is homomorphism*]

$=[\varphi(x)]^k\ \varphi(x)$ [*Assumed above*]

$=[\varphi(x)]^{k+1}$

$\therefore$ The result is true for $n=k+1$.

Thus the result is true for +ve integers.

For n=0 :

$$\varphi(x^0)=\varphi(e)=\bar{e}$$

and $\qquad \bar{e}=[\varphi(x)]^0$

$\therefore \qquad \varphi(x^0)=[\varphi(x)]^0.$

Thus the result is true for $n=0$.

When n=−m, where m is a +ve integer.

$$\varphi(x^n)=\varphi(x^{-m})=\varphi[(x^{-1})]^m=[\varphi(x^{-1})]^m$$
$$=\{[\varphi(x)]^{-1}\}^m=[\varphi(x)]^m=[\varphi(x)]^n.$$

Thus the result is true for −ve integers.

Hence the result is true for any integer.

Theorem II. *If G is a group and N is a normal sub-group of G. Define the mapping φ : $G\to G/N$ given by $\varphi(x)=Nx$ for all $x\in G$; then φ is a homomorphism of G onto G/N.*

Proof. (I) Let $\quad x, y\in$ G.

Then $\qquad \varphi(xy)=\mathrm{N}xy$ [$\because \varphi(x)=\mathrm{N}x$]

$=\mathrm{N}x\mathrm{N}y$ [$\because$ *N is a normal sub-group*]

$=\mathrm{N}x \cdot \mathrm{N}y=\varphi(x)\cdot\varphi(y)$

$\therefore$ *φ is homomorphism.*

(II) When $\mathrm{X}\in \mathrm{G/N}$, then $\mathrm{X}=\mathrm{N}y$, where $y\in$ G

$\Rightarrow \qquad \mathrm{X}=\varphi(y).$

Thus φ *is onto.*

This φ is called **natural mapping** or **canonical mapping** and is denoted by σ.

Theorem III. *If φ is a homomorphism of G into $\bar{G}$ with kernal K, then K is a normal sub-group of G.*

Proof. Let $\varphi : G \to \bar{G}$, where K is the kernal.

Non-emptiness.

We know that $\varphi(e)=\bar{e}$

$\Rightarrow$ $e \in K$ [*Def. of Kernel*]

Thus K is non-empty and $K \subset G$.

K is a sub-group of G.

For this, we have to establish that

(*i*) $\forall\ k_1, k_2 \in K \Rightarrow k_1k_2 \in K$

(*ii*) $\forall\ k_1 \in K \Rightarrow k_1^{-1} \in K.$

(*i*) $\forall\ k_1 \in K \Rightarrow \varphi(k_1)=\bar{e}$
[$\because$ $k_1 \in K \Rightarrow k_1 \in G$ *as* $K \subset G$]

$\forall k_2 \in K \Rightarrow \varphi(k_2)=\bar{e}$
[$\because$ $k_2 \in K \Rightarrow k_2 \in G$ *as* $K \subseteq G$]

Now $\varphi(k_1k_2)=\varphi(k_1)\varphi(k_2)$ [$\because$ φ *is homomorphism*]

$=\bar{e}\,.\,\bar{e}=\bar{e}$

$\Rightarrow$ $k_1k_2 \in K.$ [*Def. of Kernel*]

(*ii*) $\forall k_1 \in K \Rightarrow k_1 \in G$ [$\because$ $K \subseteq G$]

$\Rightarrow k_1^{-1} \in G$ [$\because$ *G is a group*]

Now $\varphi(k_1^{-1})=[\varphi(k_1)]^{-1}$

$=(\bar{e})^{-1}=\bar{e}$

$\Rightarrow$ $k_1^{-1} \in K$ [*Def. of Kernel*]

Thus *K* is a sub-group of G.

K is a normal sub-group of G

For this, we have to prove that

$$gk_1 g^{-1} \in K\ \forall k_1 \in K,\ \forall g \in G.$$

Now $\varphi(gk_1 g^{-1})=\varphi((gk_1)g^{-1})$

$=\varphi(gk_1)\varphi(g^{-1})$ [$\because$ φ *is homomorphism*]

$=\varphi(g)\ \varphi(k_1)\varphi\ (g^{-1})$
[$\because$ φ *is homomorphism*]

$=\varphi(g)\ \bar{e}\ \varphi(g^{-1})$

$=\varphi(g)\ \varphi(g^{-1})$

$=\varphi(g\,g^{-1})$ [$\because$ *φ is homomorphism*]

$=\varphi(e)=\bar{e}$

Thus $gk_1g^{-1}\in K$.

Hence K is a normal sub-group of G.

Theorem IV. *Let φ be a homomorphism of G into $\bar{G}$ with kernel K, prove that $G/K\simeq\bar{G}$.* **(V. Important)**

Sol. Let $a\in G$.

Then $Ka\in G/K$ and $\varphi(a)\in\bar{G}$.

Consider $\psi: G/K \to \bar{G}$ defined by

$\psi(Ka)=f(a) \quad \forall \quad a\in G,$

To Prove. *ψ is well-defined*

If $a, b\in G$ and $Ka=Kb$, then

$\psi(Ka)=\psi(Kb)$

We have : $Ka=Kb \quad \Rightarrow \quad ab^{-1}\in K$

$\Rightarrow \quad \varphi(ab^{-1})=\bar{e}$, the identity of $\bar{G}$

$\Rightarrow \quad \varphi(a)\,.\,\varphi(b^{-1})=\bar{e}$ [$\because$ *φ is homomorphism*]

$\Rightarrow \quad \varphi(a)\,.\,[\varphi(b)]^{-1}=\bar{e}$

$\Rightarrow \quad \varphi(a)\,.\,[\varphi(b)]^{-1}\,\varphi(b)=\bar{e}\,\varphi(b)$ [*Post-multiplying by $\varphi(b)$*]

$\Rightarrow \quad \varphi(a)\,.\,\bar{e}=\varphi(b)$

$\Rightarrow \quad \varphi(a)=\varphi(b)$

$\Rightarrow \quad \psi(Ka)=\psi(Kb)$

Thus ψ is well-defined.

To prove. *ψ is one-one.*

$\psi(Ka)=\psi(Kb) \quad \Rightarrow \quad \varphi(a)=\varphi(b)$

$\Rightarrow \quad \varphi(a)\,.\,[\varphi(b)]^{-1}=\varphi(b)\,.\,[\varphi(b)]^{-1}$

[*Post-multiplying by $[\varphi(b)]^{-1}$*]

$\Rightarrow \quad \varphi(a)\,.\,\varphi(b^{-1})=\bar{e}$

$\Rightarrow \quad \varphi(ab^{-1})=\bar{e}$ [$\because$ *φ is homomorphism*]

$\Rightarrow \quad ab^{-1}\in K$ [*Def. of Kernal*]

$\Rightarrow \quad Ka=Kb$

$\Rightarrow$ ψ is one-one.

To Prove. *ψ is onto.*

Let $y \in \bar{G}$, then $y = \varphi(a)$ for some $a \in G$. [$\because$ *φ is onta $\bar{G}$*]

Now $$Ka \in G/K$$

and $$\psi(Ka) = \varphi(a) = y$$

$\therefore$ ψ is onto $\bar{G}$.

To Prove. *ψ is homomorphism.*

$$\psi[(Ka)\,.\,(Kb)] = \psi(Kab) = \varphi(ab)$$
$$= \varphi(a)\,.\,\varphi(b) \qquad [\because \ \varphi \text{ is homomorphism}]$$
$$= \psi(Ka)\,.\,(Kb)$$

$\therefore$ ψ is homomorphism

Thus ψ is an isomorphism of G/K onto $\bar{G}$.

Hence $G/K \simeq \bar{G}$.

Example 49. *Let G be $(Z, +)$ i.e. the group of integers under additiona and let $f : G \to \bar{G}$ defined by $\varphi(x) = 2x \ \forall \ x \in G$ Prove that f is homomorphism. Determine its kernal.* [G.N.D.U. 1982]

Sol. Here $\varphi(x) = 2x \ \forall \ x \in G$

$$\forall \ x, y \in G \quad \Rightarrow \quad x + y \in G$$
[$\because$ *G is a group under addition*]

Now $$f(x+y) = 2(x+y)$$
$$= 2x + 2y$$
$$= f(x) + f(y)$$

Hence f is homomorphism.

Kernal of homomorphism consists of half of zero *i.e.*, the integers whose double is zero.

Thus $$K = \{0\}.$$

Example 50. *Let $\varphi : G \to \bar{G}$ defined by $\varphi(x) = \bar{e} \ \forall x \in G$. Prove that φ is homomorphism.*

Sol. $\forall \ x, y \in G \Rightarrow y \in G$ [$\because$ *G is a group*]

Now $$\varphi(xy) = \bar{e}$$
$$= \bar{e}\ \bar{e} = \varphi(x)\ \varphi(y)$$

Hence φ is homomorphism.

Sol. Let G be a cyclic group having generator a.

Then $G=\{a^n \mid n\in Z\}$ *i e.* $G\{a^0, a^1, a^2, \ldots\ldots, a^n, \ldots\ldots\}$

Let us define $\varphi: G\to Z$ by $\varphi(a^n)=n \ \forall\ a\in G$.

(*i*) **φ is one-one.**

If $\varphi(a^n)=\varphi(a^m)$, then $n=m$ and $a^n=a^m$.

$\therefore$ φ is one-one.

(*ii*) **φ is onto.**

$\forall n\in Z$, $a^n\in G$ is mapped onto n by φ.

$\therefore$ φ is onto.

(*iii*) **φ is homomorphism.**

$$\varphi(a^n \cdot a^m)=\varphi(a^{n+m})=n+m.$$

But $\quad \varphi(a^n)+\varphi(a^m)=n+m.$

$\therefore \quad \varphi(a^n \cdot a^m)=\varphi(a^n)+\varphi(a^m)$

$\therefore$ φ is homomorphism

Hence φ is an isomorphism.

Example 56. *Prove that any finite cyclic group is isomorphic to the additive group of integers modulo n.* **(V. Important)**

Sol. Let $\quad G=\{a^0, a^1, a^2, \ldots\ldots, a^{n-1}\}$

Let $\quad H=\{0, 1, 2, 3, \ldots\ldots, n-1\}$

be the group of integers under addition mod n.

Let us define $\varphi: G\to H$ by $\varphi(a^k)=k$.

φ is one-one.

Let $a^r, a^s\in G$.

The $\varphi(a^r)=\varphi(a^s) \Rightarrow r=s \Rightarrow a^r=a^s$

$\therefore$ φ is one-one.

φ is onto.

Let any $m\in H$.

Then $a^m\in G$ such that $\varphi(a^m)=m \Rightarrow \varphi$ is onto.

φ is homomorphism.

Let $\quad a^r, a^s\in G$.

Then
$$\varphi(a^r \cdot a^s)=\varphi(a^{r+s})$$
$$=\begin{cases} r+s & \text{if } r+s<n \\ r+s-n & \text{if } r+s\geqslant n \end{cases}$$
$$=\begin{cases} \varphi(a^r)+\varphi(a^s) & \text{if } r+s<n \\ \varphi(a^r)+\varphi(a^s)-\varphi(a^n) & \text{if } r+s\geqslant n \end{cases}$$
$$=\varphi(a^r)+\varphi(a^s) \qquad [\because \varphi(a^n)=0]$$

$\therefore$ φ is homomorphism.

$\therefore$ φ is isomorphism.

Hence $G\cong H$.

5. **Invariant Elements.** *The elements which are mapped onto themselves are called invariant elements.*

6. **Identity Mapping.** *If all the elements are mapped onto themselves, then mapping is called an identity mapping.*

For Ex. If $\varphi=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, then φ is an identity mapping.

7. **Cyclic Permutation.** *A permutation is said to be cyclic if each element is mapped onto the next element and the last element is mapped onto the first element.*

For Ex. If $\varphi=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, then φ is a cyclic permutation.

This can also be written as (1 2 3) and is known as a **cycle of length 3** or **3-cycle.**

8. **Equality of two Permutations.**

Two permutations f and g of degree n are said to be equal if $f(a)=g(a)\ \forall\ a\in S$, where S is a finite set of n distinct elements.

For Ex. If $f=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g=\begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

Here $f=g$.

[$\because$ *In both cases 1 is replaced by 2, 2 by 3, 3 by 4 and 4 by 1*]

Note : The interchange of columns does not change the permutation.

For Ex. If $f=\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$.

then $f=\begin{pmatrix} a_2 & a_1 & a_3 \\ b_2 & b_1 & b_3 \end{pmatrix}=\begin{pmatrix} a_1 & a_3 & a_2 \\ b_1 & b_3 & b_2 \end{pmatrix}$, etc.

9. **Product (or composite) of two Permutations.**

The product of two permutations is the composite of the two mappings.

If f and g are two permutations on a set A *i.e.*, $f: A\to A$, $g: A\to A$, then $g\,o\,f: A\to A$.

Since f and g are both one-one onto mapping,

$\therefore$ their composite gof is also one-one onto itself.

Hence gof is also a permutation.

This permutation gof is called the product of f and g.

For Ex. Let $f=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $g=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Then $g\,o\,f=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

(vi) $$P_3 \, o \, P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 3 & 1 \\ 2 & 1 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Example 59. *By the help of Ex. 58, prove that permutation multiplication is associative.*

Sol. We have to prove that $P_1 \, o \, (P_2 \, o \, P_3) = (P_1 \, o \, P_2) \, o \, P_3$.

$$P_2 \, o \, P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \text{[As in Ex. 58]}$$

$$\therefore \quad P_1 \, o \, (P_2 \, o \, P_3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \ldots(1)$$

Also $$P_1 \, o \, P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \text{[As in Ex. 58]}$$

$$\therefore \quad (P_1 \, o \, P_2) \, o \, P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 3 & 2 & 1 \\ 3 & 2 & 1 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \ldots(2)$$

From (1) and (2), $P_1 \, o \, (P_2 \, o \, P_3) = (P_1 \, o \, P_2) \, o \, P_3$.

Hence the permutation multiplication is associative.

Example 60. *For the permutations of Ex. 58, find $(P_1)^{-1}$, $(P_2)^{-1}$, $(P_3)^{-1}$, $(P_1 \, o \, P_2)$, $(P_3 \, o \, P_1)^{-1}$ and $(P_2 \, o \, P_3)^{-1}$.*

Sol. We have : $P = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

We have to find P_1^{-1} such that $P_1^{-1} \, o \, P_1 = I$

$$\therefore \qquad P_1^{-1} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

so $$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$\therefore \qquad P_2^{-1}=\begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

And $$P_3=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\therefore \qquad P_3^{-1}=\begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Now $$P_1 \circ P_2=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$ [*Ex.* 58 (*i*)]

$$\therefore \qquad (P_1 \circ P_2)^{-1}=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Also $$P_3 \circ P_1=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$ [*Ex.* 58 (*iv*)]

$$\therefore \qquad (P_3 \circ P_1)^{-1}=\begin{pmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

And $$P_2 \circ P_3=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$ [*Ex.* 58 (*v*)]

$$\therefore \qquad (P_2 \circ P_3)^{-1}=\begin{pmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

CAYLEY'S THEOREM

Statement. *Every finite group is isomorphic to a sub-group of the group of permutation group.* [Pbi. U. 1975]

Proof. Let $A(G)=\{\sigma : \sigma : G \to G$, one-one, onto mapping$\}$.

Let $\Gamma g : G \to G$ defined by $x\Gamma g = xg \quad \forall\ x \in G$.

To prove. $\Gamma g \in A(G)$

i.e., Γg is one-one, onto

Γg is one-one

$\forall\ x, y \in G$, $x \neq y$, G, if possible, let their images be same

i.e., let $\qquad x\Gamma g = y\Gamma g$

$\Rightarrow \qquad xg = yg$

$\Rightarrow \qquad x = y,$ [*By Cancellation Law*]

which is a contradiction. [$\because\ x \neq y$]

$\therefore \qquad x\Gamma g \neq y\Gamma g$

Thus different elements have different images.

Hence Γg is one-one.

Γg is onto.

$\forall z \in G, g \in G \Rightarrow g^{-1} \in G$ [$\because$ *G is a group*]

$\Rightarrow \quad zg^{-1} \in G$

Now $\quad zg^{-1}\Gamma g = zg^{-1}g = z$

$\therefore \quad \Gamma g$ is onto.

Hence $\quad \Gamma g \in A(G)$

Now let $H = \{\Gamma g ; \Gamma g : G \to G$ defined by $x\Gamma g = xg \ \forall\ x \in G\}$

$H \subset A(G)$ [$\because$ *All elements* $\in$ *H will* $\in$ *A(G)*]

To prove. **H is a sub-group of A(G).**

i.e., we have to prove that

(*i*) $\forall\ \Gamma g, \Gamma h \in H \quad \Rightarrow \quad \Gamma g\,\Gamma h \in H$, where $g, h \in G$

(*ii*) $\forall\ \Gamma g \in H \quad \Rightarrow \quad \Gamma g^{-1} \in H \quad \forall\ g \in G.$

Proof. (*i*) Since $\Gamma g : G \to G$ and $\Gamma h : G \to G$

$\therefore$ Resultant of Γg and Γh is possible.

$\therefore \quad \Gamma g\,\Gamma h : G \to G$

Also $\quad g, h \in G \quad \Rightarrow \quad gh \in G$ [$\because$ *G is a group*]

$\Rightarrow \quad \Gamma gh \in H$ ...(1)

To prove. $\Gamma gh = \Gamma g\,\Gamma h.$

Proof. Consider $\forall\ x \in G$, then $x\,\Gamma gh = xgh.$

Also $\quad x\Gamma g\,\Gamma h = (x\,\Gamma g)\Gamma h$

$= (xg)\,\Gamma h = (xg)h = xgh$

$\therefore$ Image of x under Γgh and $\Gamma g\,\Gamma h$ is same

Hence $\quad \Gamma g\,\Gamma h = \Gamma gh$ ...(I)

But $\quad \Gamma gh \in H$ [*From* (*1*)]

Hence $\quad \Gamma g\,\Gamma h \in H.$

$\therefore$ 1st condition for sub-group is satisfied.

(*ii*) Now $\quad g \in G \quad \Rightarrow \quad g^{-1} \in G$ [$\because$ *G is a group*]

$\therefore \quad \Gamma g^{-1} \in H$ ...(2)

To prove. $\Gamma g^{-1} = \Gamma g^{-1}.$

Proof. If $\Gamma g : G \to G$ is one-one, onto

$\therefore$ Inverse mapping *i.e.* Γg^{-1} is justified.

Also Γg^{-1} will be one-one onto.

and $\Gamma g^{-1} : G \to G$ is one-one, onto

$\forall\ x \in G,\ x\,\Gamma g = xg$

Since inverse mapping exists, $\therefore \quad xg\Gamma\, g^{-1} = x$

Again $\quad xg\Gamma g^{-1} = (xg)g^{-1} = xgg^{-1} = xe = x$

$\therefore$ Image of xg under Γg^{-1} and Γg^{-1} is same.

$\therefore \quad \Gamma g^{-1} = \Gamma g^{-1}$

But $\quad \Gamma g^{-1} \in H$ *[From (2)]*

$\therefore \quad \Gamma g^{-1} \in H$

$\therefore$ 2nd condition for sub-group is satisfied.

$\therefore$ H is a sub-group of A(G).

Hence H is a group in itself.

To prove. $\quad G \simeq H.$

Proof. Let $\psi : G \to H$ defined by $\psi(g) = \Gamma g \ \forall \ g \in G$

ψ is onto.

$\forall \ g \in H, \exists \ g \in G$ such that $\psi(g) = \Gamma g$.

$\therefore$ ψ is onto.

ψ is one-one.

$\forall \ g \neq h \in G$, if possible, let their images be same

i.e., let $\quad \psi(g) = \psi(h)$

$\Rightarrow \quad \Gamma g = \Gamma h$ ...(3)

Now $\quad \Gamma g : G \to G \quad$ and $\quad \Gamma h : G \to G$

Consider $\forall \ x \in G, \ x\Gamma g = xg, \ x\Gamma h = xh$

$\therefore$ From (3), $\quad \Gamma g = \Gamma h$

$\Rightarrow \quad x\Gamma g = x\Gamma h$

$\Rightarrow \quad xg = xh$

$\Rightarrow \quad g = h,$ *[By Cancellation Law]*

which is a contradiction $[\because \ g \neq h]$

$\therefore \quad \Gamma g \neq \Gamma g \quad \Rightarrow \quad \psi(g) \neq \psi(h)$

$\Rightarrow$ different elements have different images

$\therefore$ ψ is one-one.

ψ is homo-morphism.

i.e. we have to prove that $\psi(gh) = \psi(g)\psi(h)$.

$$\psi(gh) = \Gamma gh$$
$$= \Gamma g \ \Gamma h \quad \text{[From I]}$$
$$= \psi(g) \ \psi(h)$$

$\therefore$ ψ is homomorphism.

Hence $\quad G \simeq H.$

CENTRE OF A GROUP

Definition. *The centre of a group G is the set of those elements of G which commute with every element of G.*

This is generally denoted by **Z**.

Thus $\quad Z = \{y \in G \mid zx = xz \ \forall \ x \in G\}.$

Prove that the centre Z of a group G is a normal sub-group of G.

Proof. Clearly $Z \subset G$.

[$\because$ *all the elements of Z belong to G*]

Non-emptiness.

It contains at least identity element

$\because \quad ex = gx \quad \forall\, x \in G$

$\therefore$ e is commutative with all the elements of G.

$\therefore \quad e \in Z.$

Thus Z is non-empty.

Sub-group.

For this, we have to prove that

(i) $\forall\, z_1, z_2 \in Z \Rightarrow z_1 z_2 \in Z$

(ii) $\forall\, z_1 \in Z \Rightarrow z_1^{-1} \in Z.$

(i) $z_1 \in Z \Rightarrow z_1 x = x z_1 \quad \forall\, x \in G$

$z_2 \in Z \Rightarrow z_2 x = x z_2 \quad \forall\, x \in G$

Now $z_1 z_2 x = z_1(z_2 x) = z_1(x z_2)$ [$\because z_2 x = x z_2$]

$= (z_1 x) z_2 = (x z_1) z_2$ [$\because z_1 x = x z_1$]

$= x z_1 z_2$

$\Rightarrow$ $z_1 z_2$ is commutative with $x \quad \forall\, x \in G$

$\Rightarrow$ $z_1 z_2 \in Z.$

(ii) $z_1 \in Z \Rightarrow z_1 x = x z_1 \quad \forall\, x \in G$

$\Rightarrow z_1^{-1} z_1 x = z_1^{-1} x z_1$ [*Operating by* z_1^{-1} *on left*]

$\Rightarrow ex = z_1^{-1} x z_1$

$\Rightarrow x = z_1^{-1} x z_1$

$\Rightarrow x z_1^{-1} = z_1^{-1} x z_1 z_1^{-1}$

[*Operating by* z_1^{-1} *on right*]

$\Rightarrow x z_1^{-1} = x_1^{-1} x e$

$\Rightarrow x z_1^{-1} = z_1^{-1} x$

$\Rightarrow$ z_1^{-1} is commutative with $x \quad \forall\, x \in Z$

$\Rightarrow \quad z_1^{-1} \in Z$

Thus Z is a sub-group of G.

Normal sub-group.

For this we have to prove that

$g z_1 g^{-1} \in Z \quad \forall\, g \in G, z_1 \in Z$

$g z_1 g^{-1} = (g z_1)\, g^{-1}$

$= (z_1 g)\, g^{-1}$ [$\because g z_1 = z_1 g$]

$= z_1 g g^{-1}$

$= z_1 e$ [$\because g g^{-1} = e$]

$= z_1 \in Z$

$\therefore \quad g z_1 g^{-1} \in Z.$

Hence Z is a normal sub-group of G.

NORMALIZER

Definition. *If $a \in G$, then normalizer of a in G is the set of all those elements of G which commute with a.*

This is generally denoted by $N(a)$.

Thus $N(a)=\{x \in G) \mid ax=xa\}$.

Prove that normalizer N(a) of a∈Z is a sub-group of G.

Proof. Clearly $N(a) \subset G \ \forall a \in G$.

[$\because$ *all the elements of N(a) belong to G*]

Non-emptiness.

$\because \ ea=ae=a \qquad \therefore \ e \in N(a)$

$\Rightarrow$ $N(a)$ is non-empty. [$\because$ *at least identity* $\in N(a)$]

Sub-group.

For this, we have to prove that

(*i*) $\forall x, y \in N(a) \Rightarrow xy \in N(a)$

(*ii*) $\forall x \in N(a) \Rightarrow x^{-1} \in N(a)$.

(*i*) $x \in N(a) \Rightarrow xa=ax$ ...(1)

$y \in N(a) \Rightarrow ya=ay$ ...(2)

$$(xy)a=x(ya)$$
$$=x(ay) \qquad [\because \text{ of } (2)]$$
$$=xay=(xa)y$$
$$=(ax)y \qquad [\because \text{ of } (1)]$$
$$=a(xy)$$
$$\Rightarrow \quad xy \in N(a).$$

(*ii*) $x \in N(a) \Rightarrow xa=ax$

$\Rightarrow \quad xax^{-1}=axx^{-1}$ [*Operating by x^{-1} on right*]

$\Rightarrow \quad xax^{-1}=ae=a$

$\Rightarrow \quad x^{-1}xax^{-1}=x^{-1}a$ (*Operating by x^{-1} on left*]

$\Rightarrow \quad eax^{-1}=x^{-1}a$

$\Rightarrow \quad ax^{-1}=x^{-1}a$

$\Rightarrow \quad x^{-1} \in N(a)$

Hence $N(a)$ is a sub-group of G.

Particular Case. $N(e)=\{x \in G \mid xe=ex\}$

To prove. $N(e)=G$.

i.e., all the elements of G are commutative with e.

$\forall \ g \in G, \quad ge=eg$. [$\because$ *e is the identity of G*]

$\Rightarrow \quad g \in N(e)$

$\Rightarrow \quad g \in N(e)$

III. **Transitivity** *i.e.,* $a \sim b,\ b \sim c \Rightarrow a \sim c$.

$a \sim b \Rightarrow a = x^{-1}bx$ for some $x \in G$

$b \sim c \Rightarrow b = y^{-1}cy$ for some $y \in G$

$\therefore \quad a = x^{-1}(y^{-1}cy)x$ [*Putting the value of b in first*]

$= (x^{-1}y^{-1})c(yx) = (yx)^{-1}c(yx)$ where $yx \in G$

$\Rightarrow \quad a \sim c$

Thus $\sim$ is transitive.

Hence $\sim$ is an equivalence relation.

ADDITIONAL EXAMPLES

(V. Important)

Example 63. *Prove that the order of a cyclic group is equal to the order of its generator.*

Sol. Let $G = \langle a \rangle$ be a cyclic group whose generator is a.

Let $O(a) = m$, where m is a finite integer.

$\therefore \quad e = a^0, a^1, a^2, \ldots\ldots\ldots, a^{m-1} \in G.$

To prove. $a^0, a^1, a^2, \ldots\ldots\ldots, a^{m-1}$ *are the only elements of G.*

Let $a^i = a^j$, where $i, j \leqslant m-1$

$\Rightarrow \quad a^{i-j} = e$, where $0 < i-j < m$,

which is a contradiction.

Thus $a^i \neq a^j$ for any i, j.

Consider $a^r \in G$.

Then $r = mq + s$, where $0 \leqslant s < m$ [*Euclid's Algorithm*]

$\therefore \quad a^r = a^{mq+s} = a^{mq}a^s = (a^m)^q a^s = e^q a^s$ [*By def.*]

$= ea^s = a^s$.

But a^s is one amongst $a^0, a^1, a^2, \ldots\ldots\ldots, a^{m-1}$.

Consequently, $a^r \in G$, which is again equal to one of the elements.

$a^0, a^1, a^2, \ldots\ldots\ldots, a^{m-1}$.

Hence $O(G) = O(a) = m$.

Example 64. *Prove that every group of order three a cyclic.* [G N.D U. 1975 S]

Sol. Let $O(G) = 3$.

Let $a \neq e \in G$.

Consider a sub-group generated by a.

Let $H = \langle a \rangle$.

Then $O(H) > 1$ [$\because$ $H = \langle a \rangle \Rightarrow a \in H$
Also $e \in H \Rightarrow O(H) > 1$]

By Lagrange's Theorem, $O(H)/O(G)$

$\Rightarrow \quad O(H)/3$

$\Rightarrow \quad O(H)=1$ or 3 [$\because$ *3 is prime*]

But $\quad O(H)>1 \quad \therefore \quad O(H)\neq 1$

Hence $\quad O(H)=3=O(G)$

$\Rightarrow \quad G=H.$

But H is a cyclic group.

$\therefore$ G is also cyclic group.

Hence the result.

Example 65. *Show that every group of order three must be abelian.* **(V. Important)** [G.N.D.U. 1982]

Sol We know that every cyclic group must be abelian.

But the group of order three is cyclic. [*Ex. 64*]

$\therefore$ The group of order three is abelian.

Hence the result.

3

Rings

DEFINITIONS

1. Ring. [*G.N.D.U. 1981*]

A system $< R, +, . >$, *where R is a non-empty set and addition* $(+)$, *multiplication* $(.)$ *are two binary compositions on R, is called a ring if it satisfies the following postulates :*

Under Addition

(*i*) **Closure Axiom.** $\forall a, b \in R \Rightarrow a+b \in R$

(*ii*) **Associative Law.** $a+(b+c)=(a+b)+c \;\; \forall a, b, c \in R$

(*iii*) **Existence of Identity.** *There exists an element* $o \in R$, *called the* **identity under addition**, such that

$$a+0=a=0+0 \;\; \forall a \in R.$$

[0 is also called the **zero-element**]

(*iv*) **Existence of Inverse.** $\forall \; a \in R$, *there exists an element* $a \in R$, *called* **the inverse of a under addition,** *such that*

$$a+(-a)=0=(-a)+a.$$

(*v*) **Commutative Law.** $\forall a, b \in R, a+b=b+a.$

Under Multiplication

(*vi*) **Closure Axiom.** $\forall a, b \in R \Rightarrow a . b \in R.$

(*vii*) **Associative Law.** $a . (b . c)=(a . b) . c \;\; \forall a, b, c \in R.$

(*viii*) **Distributive Law.** $\forall a, b, c \in R,$

(*I*) $a . (b+c)=a . b+a . c$ **[Left]**

(*II*) $(b+c) . a=b . a+c . a$ **[Right]**

Conclusion. (*i*) **R forms an abelian group under addition**

(*ii*) **R is a semi-group under multiplication**

(*iii*) **R satisfies distributive Laws.**

Note. The ring is called **non-associative** if associative law under multiplication does not hold.

2. Commutative Ring or Abelian Ring.

In addition to the above eight postulates, the following postulate is also satisfied, the ring R is called a Commutative or an Abelian Ring.

(*ix*) **Commutative Law.** $\forall a, b \in R, a . b=b . a$

3. Ring with Unity

A ring R which contains the multiplicative identity (called unity) is called a ring with unity.

Thus if $1 \in R$ such that $a.1 = a = 1.a \ \forall a \in R$, then the ring is called a ring with unity.

4. Ring without Unity

A ring R which does not contain multiplicative identity is called a ring without unity.

5. Finite and Infinite Ring

If the number of elements in the ring R is finite, then $<R, +, .>$ is called a finite ring, otherwise it is called an infinite ring.

6. Order of Ring

The number of elements in a finite ring is called the order of the ring.

This is denoted by O(R) or $|R|$.

7. Units of a ring with unity

The elements which possess inverses under the second operation (.) are called units of a ring.

In the set I of integers, we know that $(-1)(-1)=1$.

Thus -1 is the **unit** but not **unity** of the ring.

Again $1 . 1 = 1$.

Thus 1 is the **unit** as well as **unity** of the ring.

Note. Unity is a unit but every unit is not a unity.

8. Zero divisors of a ring

Let $<R, +, .>$ be a ring.

$\forall a, b \in R$, where $a \neq 0$, $b \neq 0$.

If $ab = 0$, then R is called **a ring with zero divisors.**

Here a is called the **left-zero divisor** and b is called the **right-zero divisor.**

An element which is left as well as right-zero divisors is called the **zero divisor of the ring.**

In abelian rings, every left-zero divisor is also the right-zero divisor and vice-versa.

In non-abelian rings, there may be some elements which are simply left-zero divisors or simply right-zero divisors.

9. Ring without zero-divisor

The ring which is not with zero divisor is called the ring without zero divisor.

i.e. if $a \neq 0$, $b \neq 0$, then $ab \neq 0$.

Example 1. *Prove that $<Z,+,.>$, where Z is a set of all integers, is a ring.*

Sol. The system is $<Z,+,.>$, where

$$Z=\{\ldots\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$$

and '+' and '.' are binary compositions in Z.

Under Addition :

(*i*) **Closure Axiom.** $\forall a, b \in Z \Rightarrow a+b \in Z$

[$\because$ *sum of two integers is an integer*]

(*ii*) **Associative Law.** $a+(b+c)=(a+b)+c \ \forall a, b, c \in Z$.

(*iii*) **Existence of Identity.** There exists an element $0 \in Z$ such that $a+0=a=0+a \ \forall a \in Z$.

(*iv*) **Existence of Inverse.** $\forall a \in Z$, there exists an element $-a \in Z$

such that $a+(-a)=0=(-a)+a$.

(*v*) **Commutative Law.** $\forall a, b \in Z$, $a+b=b+a$.

Under Multiplication :

(*vi*) **Closure Axiom.** $\forall a, b \in Z \Rightarrow a \cdot b \in Z$.

[$\because$ *product of two integers is an integer*]

(*vii*) **Associative Law.** $a \cdot (b \cdot c)=(a \cdot b) \cdot c \ \forall a, b, c \in Z$.

(*viii*) **Distributive Laws** $\forall a, b, c \in Z$,

(I) $a \cdot (b+c)=a \cdot b+a \cdot c$

(II) $(b+c) \cdot a=b \cdot a+c \cdot a$

Hence $<Z, +, .>$ is a ring.

Example 2. (*i*) *Prove that $<E, +, .>$, where E is a set of even integers, is a ring.*

(*ii*) *Prove that $<M, +, .>$, where M is a set of those integers which are multiples of 5, is a ring.*

Sol. Please try yourself.

Example 3. *Prove that $<Q, +, .>$, where Q is a set of all rational numbers, is a ring.*

Sol. The system is $<Q, +, .>$, where Q is a set of rational numbers and '+' and '.' are binary compositions in Q.

Under Addition :

(*i*) **Closure Axiom.** $\forall a, b \in Q \Rightarrow a+b \in Q$.

[$\because$ *Sum of two rational numbers is a rational number*]

(*ii*) **Associative Law.** $a+(b+c)=(a+b)+c \ \forall a, b, c \in Q$.

(*iii*) **Existence of Identity.** There exists an element $0 \in Q$ such that $a+0=a=0+a \ \forall a \in Q$.

(*iv*) **Existence of Inverse.** $\forall a \in Q$, there exists an element $-a \in Q$

such that $a+(-a)=0=(-a)+a$.

(*v*) **Commutative Law.** $\forall a, b \in Q$, $a+b=b+a$.

Under Multiplication

(*vi*) **Closure Axiom.** $\forall a, b \in Q \Rightarrow a.b \in Q$.

[$\because$ *Product of two rational numbers is a rational number*]

(*vii*) **Associative Law.** $a.(b.c)=(a.b).c \ \forall a, b, c \in Q$.

(*viii*) **Distributive Laws.** $\forall a, b, c \in Q$,

(I) $a.(b+c)=a.b+a.c$

(II) $(b+c).a=b\,a+c.a$

Hence $<Q, +, .>$ is a ring.

Example 4. *Prove that* $<R, +, .>$, *where R is a set of all real numbers, is a ring.*

Sol. Please try yourself.

Example 5. *The set of all square matrices with matrix addition and matrix multiplication as compositions forms a ring when the elements are form the real (complex) field*

Sol. Please try yourself.

Example 6. *The set of residue classes modulo the positive integer m is a ring with respect to addition and multiplication of residue classes modulo m.*

Sol. The set R of residue classes modulo m is

$$R=[\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \ldots\ldots \{m-1\}].$$

Addition is defined by

$$\{r_1\}+\{r_2\}=\{r_1+r_2\} \in R,$$

where r_1+r_2 is reduced modulo m

and $$\{r_1\} . \{r_2\}=\{r_1 r_2\} \in R$$

where $r_1 r_2$ is reduced modulo m.

The zero element is $\{0\}$, which is the identity.

Example 7. *Prove that the set* $R=\{0, 1, 2, 3, 4, 5\}$ *is a commutative ring with respect to the operations of addition (mod 6) and multiplication (mod 6).* **[G.N.D.U. 1982]**

Sol. The composition (+) table is

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(*i*) Since all possible sums belong to R, therefore, R is closed w.r.t. addition (mod 6).

(*ii*) Associative law holds because $a+(b+c)=(a+b)+c$ $=a+b+c$ under addition (mod 6).

(*iii*) Here 0 is the additive identity because $a+0=a=0+a$ (mod 6).

(*iv*) From the table, we see that

$(0)^{-1}=0$. $(1)^{-1}=5$, $(2)^{-1}=4$, $(3)^{-1}=3$, $(4)^{-1}=2$ and $(5)^{-1}=1$.

$\therefore$ The inverse of every element exists.

(*v*) Commutative law holds because $a+b=b+a$ (mod 6).

The composition ($\times$) table is

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(*vi*) From the composition table it is clear that R is closed for multiplication.

(*vii*) Associative law holds because $a\times(b\times c)=(a\times b)\times c$ $=a\times b\times c$ under multiplication (mod 6).

(*viii*) $a\times(b+c)=a\times[b+c]$,

where $[b+c]$ is the least non-negative remainder obtained when $b+c$ is divided by 6

$$=[a(b+c)] \text{ reduced modulo } 6$$
$$=[ab+ac]$$
$$=[ab]+[ac]$$
$$=(a\times b)+(a\times c).$$

Thus R is a ring.

(*ix*) Commutative law holds because $a.b=b.a$ (mod 6).

Hence R is a commutative ring.

Example 8. *Prove that the set R of numbers of the form $a+b\sqrt{2}$, where a and b are integers, is a ring with respect to ordinary addition and multiplication.* **(Important)** **[Meerut 1969 S]**

Sol. Let x_1, x_2, x_3 be any three elements of the given set.

Then $x_1=a_1+b_1\sqrt{2}$, $x_2=a_2+b_2\sqrt{2}$, $x_3=a_3+b_3\sqrt{2}$.

Under Addition:

(*i*) **Closure Axiom.**

$$x_1+x_2=(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})$$
$$=(a_1+a_2)+(b_1+b_2)\sqrt{2}=a+b\sqrt{2}$$

$\therefore$ x_1+x_2 also belongs to the given set

[$\because$ $a_1+a_2=a$ *and* $b_1+b_2=b$]

(*ii*) **Associative Law.**

$$(x_1+x_2)+x_3=[(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})]+(a_3+b_3\sqrt{2})$$
$$=[(a_1+a_2)+(b_1+b_2)\sqrt{2}]+(a_3+b_3\sqrt{2})$$
$$=[\{(a_1+a_2)+a_3\}+\{(b_1+b_2)+b_3\}\sqrt{2}]$$
$$=[\{a_1+(a_2+a_3)\}+\{b_1+(b_2+b_3)\}\sqrt{2}]$$
$$=(a_1+b_1\sqrt{2})+[(a_2+b_2\sqrt{2})+(a_3+b_3\sqrt{2})]$$
$$=x_1+(x_2+x_3).$$

(*iii*) **Existence of Identity.**

The real number zero is the additive identity.

[$\because$ $0=0+0\sqrt{2}$]

(*iv*) **Existence of Inverse**

Corresponding to each number $a+b\sqrt{2}$ of the given set we have a member $-a+(-b)\sqrt{2}$ such that

$$(a+b\sqrt{2})+(-a)+(-b)\sqrt{2}=(a-a)+(b-b)\sqrt{2}$$
$$=0+0\sqrt{2}.$$

Thus $(-a)+(-b)\sqrt{2}$ is the additive inverse of $a+b\sqrt{2}$.

Hence additive inverse of each member exists in the given set.

(*v*) **Commutative Law.**

$$x_1+x_2=(a_1+a_2)+(b_1+b_2)\sqrt{2}$$
$$=(a_2+a_1)+(b_2+b_1)\sqrt{2}$$

[$\because$ *Addition of real numbers is commutative*]

$$=(a_2+b_2\sqrt{2})+(a_1+b_1\sqrt{2})$$
$$=x_2+x_1.$$

Under Multiplication:

(*vi*) **Closure Axiom.**

$$x_1x_2=(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})$$
$$=(a_1a_2+2b_1b_2)+(a_1b_2+b_1a_2)\sqrt{2}.$$

Since $a_1a_2+2b_1b_2$ and $a_1b_2+b_1a_2$ are real numbers,

$\therefore$ x_1x_2 also belongs to the given set.

(vii) Associative Law.

$$(x_1 . x_2) . x_3 = [(a_1+b_1\sqrt{2}).(a_2+b_2\sqrt{2})].(a_3+b_3\sqrt{2})$$
$$=[(a_1a_2+2b_1b_2)+(b_1a_2+b_2a_1)\sqrt{2}].(a_3+b_3\sqrt{2})$$
$$=(a_1a_2+2b_1b_2)a_3+2(b_1a_2+b_2a_1)b_3$$
$$+(b_1a_2+a_1b_2)a_3\sqrt{2}+(a_1a_2+2b_1b_2)b_3\sqrt{2}$$

Similarly this also equals $x_1.(x_2.x_3)$

(viii) Distributive Laws.

$$x_1.(x_2+x_3)=(a_1+b_1\sqrt{2}).[(a_2+b_2\sqrt{2})+(a_3+b_3\sqrt{2})]$$
$$=(a_1+b_1\sqrt{2}).[(a_2+a_3)+(b_2+b_3)\sqrt{2}]$$
$$=a_1(a_2+a_3)+a_1(b_2+b_3)\sqrt{2}+b_1\sqrt{2}(a_2+a_3)$$
$$+b_1\sqrt{2}(b_2+b_3)\sqrt{2}$$
$$=[(a_1a_2+2b_1b_2)+(a_1b_2+b_1a_2)\sqrt{2}]$$
$$+[(a_1a_3+2b_1b_3)+(a_1b_3+b_1a_3)\sqrt{2}]$$
$$=x_1.x_2+x_1.x_3.$$

Similarly $(x_2+x_3).x_1=x_2.x_1+x_3.x_1$

Hence the given set is a ring.

Example 9. *Prove that the set of matrices of order 2×2 forms a ring w.r.t. addition and multiplication of matrices.*

(V. Important)

Sol. Let S be the set of given matrices.

Let A, B, C be any three elements of S such that

$$A=\begin{bmatrix} 0 & a_1 \\ 0 & b_1 \end{bmatrix},\ B=\begin{bmatrix} 0 & a_2 \\ 0 & b_2 \end{bmatrix},\ C=\begin{bmatrix} 0 & a_3 \\ 0 & b_3 \end{bmatrix},$$

where a_1, b_1 ; a_2, b_2 ; a_3, b_3 are real numbers.

Under Addition :

(i) Closure Axiom.

$$A+B=\begin{bmatrix} 0 & a_1 \\ 0 & b_1 \end{bmatrix}+\begin{bmatrix} 0 & a_2 \\ 0 & b_2 \end{bmatrix}=\begin{bmatrix} 0 & a_1+a_2 \\ 0 & b_1+b_2 \end{bmatrix}=\begin{bmatrix} 0 & a' \\ 0 & b' \end{bmatrix}$$

Since $a_1+a_2=a'$ and $b_1+b_2=b'$ also belong to R,

$$\therefore\quad \begin{bmatrix} 0 & a' \\ 0 & b' \end{bmatrix}\in S.$$

$\therefore$, S is closed w.r.t. addition.

(ii) Associative Law.

We know that addition of matrices is associative. *[Verify !]*

(iii) Existence of Identity

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the zero element of S.

(*iv*) **Existence of Inverse.**

Additive inverse of $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \in S$ is $\begin{bmatrix} 0 & -a \\ 0 & -b \end{bmatrix}$

because $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}+\begin{bmatrix} 0 & -a \\ 0 & -b \end{bmatrix}=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Obviously $\begin{bmatrix} 0 & -a \\ 0 & -b \end{bmatrix} \in S$ as $-a, -b \in R$.

Thus additive inverse of every element of S exists in S.

(*v*) **Commutative Law**

We know that addition of matrices commutative [*Verify* !]

Under Multiplication :

(*vi*) **Closure Axiom.**

$$A.B=\begin{bmatrix} 0 & a_1 \\ 0 & b_1 \end{bmatrix}\cdot\begin{bmatrix} 0 & a_2 \\ 0 & b_2 \end{bmatrix}=\begin{bmatrix} 0 & a_1b_2 \\ 0 & b_1b_2 \end{bmatrix}$$

Since a_1b_2 and $b_1b_2 \in R$, $\therefore$ $A.B \in S$.

$\therefore$ S is closed w.r.t. multiplication.

(*vii*) **Associative Law.**

We know that multiplication of matrices is associative. [*Verify* !]

(*viii*) **Distributive Laws.**

We know that multiplication of matrices is distributive w.r.t. addition.

Hence the given system is a ring.

Example 10. *Give an example of the following :*

(*i*) *A commutative ring without unity.*
(*ii*) *A non-commutative ring with unity.*
(*iii*) *A ring with zero divisors.*
(*iv*) *A non-commutative ring.* **[Pbi. U. 1978]**

Sol. (*i*) The ring of even integers is a commutative ring without unity.

(*ii*) The ring of 2×2 matrices over reals is a non-commutative ring with unity.

(*iii*) The ring of 2×2 matrices is a ring such that

$$[A]\neq O, [B]\neq 0 \quad \text{still} \quad AB=O.$$

(*iv*) The ring of matrices is non-commutative.

Example 11. *If* $a, b, c, d \in R$, *evaluate* $(a+b)(c+d)$.

Sol. $(a+b)(c+d)=a(c+d)+b(c+d)$ [*Right Distributive Law*]

$=ac+ad+bc+bd.$ [*Left Distributive Law*]

Example 12. *Prove that if $a, b \in R$, then*

$$(a+b)^2 = a^2+ab+ba+b^2,$$

where by x^2 we mean xx.

Sol. $(a+b)^2 = (a+b)(a+b)$

$= a(a+b)+b(a+b)$ [*Right Distributive Law*]

$= (aa+ab)+(ba+bb)$ [*Left Distributive Law*]

$= a^2+ab+ba+b^2.$

Example 13. (*i*) *If $a^2 = a \ \forall \ a \in R$, then $a+a=0$.*

(*ii*) *If every $x \in R$ satisfies $x^2 = x$, prove that R must be commutative.* **[G.N.D.U. 1981]**

Sol. (*i*) $(a+a)^2 = (a+a)$ [*Given*]

$\Rightarrow (a+a)(a+a) = a+a$

$\Rightarrow a^2+a^2+a^2+a^2 = a+a$ [*Distributive Laws*]

$\Rightarrow a+a+a+a = a+a$

$\Rightarrow a+a=0.$ [*Cancellatian Laws*]

(*ii*) Let $a, b \in R \Rightarrow a+b \in R$

We have $(a+b)^2 = a+b$

$\Rightarrow a^2+ab+ba+b^2 = a+b$

$\Rightarrow a+ab+ba+b = a+b$ [$\because$ $a^2 = a$ and $b^2 = b$]

$\Rightarrow (a+b)+(ab+ba) = a+b$

$\Rightarrow ab+ba = 0$ [*Cancellation Laws*]

$\Rightarrow ab+ba = ab+ba$

$\Rightarrow ba = ab$ [*Left Cancellation Law*]

$\Rightarrow$ R is commutative.

Example 14. *If R is a system satisfying all the conditions for a ring with unit element with the possible exception $a+b=b+a$, prove that R is a ring.*

Sol. $(a+b).(1+1) = (a+b).1+(a+b).1$

$= a.1+b.1+a.1+b.1$

$= a+(b+a)+b$

Again $(a+b).(1+1) = a.(1+1)+b.(1+1)$

$= a.1+a.1+b.1+b.1$

$= a+(a+b)+b$

Then $a+(b+a)+b = a+(a+b)+b$ [*By Distributive Law*]

$\Rightarrow b+a = a+b$

$\Rightarrow$ addition is commutative.

Hence R is a ring.

PROPERTIES OF RINGS

Let $<R, +, .>$ *be a ring, then* $\forall a, b \in R$,

(*i*) $a \cdot 0 + 0 \cdot a = 0$, *where 0 is additive identity.*

(*ii*) $a(-b) = -(ab) = (-a)b$.

(*iii*) $(-a)(-b) = ab$.

Proof. (*i*) $\forall a \in R$,

$$a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$$ [*By Right Distributive Law*]

$\Rightarrow$ $0 = a \cdot 0$ [*By right cancellation since R is a group under addition*]

$\Rightarrow$ $a \cdot 0 = 0$

Similarly $0 \cdot a = 0$

Hence $a \cdot 0 = 0 \cdot a = 0$

(*ii*) $a[b+(-b)] = a \cdot 0 = 0$ [*By part* (*i*)]

$\Rightarrow$ $ab + a(-b) = 0$

$\Rightarrow$ $a(-b) = -(ab)$

Similarly $(-a)b = -(ab)$

Hence $a(-b) = -(ab) = (-a)b$.

(*iii*) $(-a)(-b) = -[(-a)b] = -[1-(ab)]$

$=$ inverse of (inverse of ab)

$= ab$.

Example 15. *If R is a ring with unity element 1, then*

(*i*) $(-1) \cdot a = -a = a \cdot (-1)$

(*ii*) $(-1) \cdot (-1) = 1$.

Sol. (*i*) $[1+(-1)] \cdot a = 1 \cdot a + (-1) \cdot a$ [*Right Distributive Law*]

$\Rightarrow$ $0 \cdot a = a + (-1) \cdot a$

$\Rightarrow$ $0 = a + (-1) \cdot a$

$\therefore$ $(-1) \cdot a = -a$

Similarly $a \cdot (-1) = -a$

(*ii*) $(-1) \cdot (-1) = -(-1)$ [*By part* (*i*)]

$=$ inverse of (inverse of 1)

$= 1$.

CANCELLATION LAWS IN A RING

Let $<R, +, .>$ be a ring.

Since $<R, +, .>$ is an abelian group, therefore, cancellation laws for addition hold good.

Remember. A ring R is an integral domain if

(I) **R is commutative**

(II) **R has unity element.**

(III) **R is without zero divisors.**

Illustrations :

(I) Ring of integers is an integral domain.

(II) Ring of numbers $a+ib$, where $a, b \in Z$, is an integral domain.

(III) Ring of numbers $a+b\sqrt{2}$, where $a, b \in Z$ is an integral domain.

(IV) The ring of even integers with zero is not an integral domain since it does not contain the unity element 1 such that

$$a \cdot 1 = 1 \cdot a = a$$

though it does not have zero divisors.

(*iii*) **Field.** *A ring R is said to be a field if it has at least two elements and* (*i*) *is commutative* (*ii*) *has unity* (*iii*) *every non-zero element of R is inversible w.r.t. multiplication.* **[G N.D.U. 1981]**

Illustrations.

(I) Ring of rational numbers, ring of real numbers and ring of complex numbers are fields.

(II) Each commutative division ring is a field.

(III) Set of integers under addition

$\equiv$(mod 5) and multiplication

$\equiv$(mod. 5) is a finite field having 5 elements

$[\{0\}, \{1\}, \{2\}, \{3\}, \{4\}]$.

Inverse of $\{2\}$ is $\{3\}$ because $\{2\} \times \{3\} = \{1\}$

Inverse of $\{1\}$ is $\{1\}$

Inverse of $\{4\}$ is $\{4\}$.

(IV) Set of integers under addition

$\equiv$(mod 6) and multiplication

$\equiv$(mod 6) is not a field but a ring.

(V) Set of integers under addition

$\equiv$(mod p) and multiplication

$\equiv$(mod p) is a field iff p is prime.

Theorem I. *A finite integral domain D is a field.*

(Important) [G.N.D.U. 1981 ; Pbi. U. 1977]

Proof. Let $x_1, x_2, \ldots\ldots, x_n$ be all n distinct elements of D.

If $a \in D$, where $a \neq 0$,

then $x_i a \in D$ for $i=1, 2, 3, \ldots\ldots, n$ and all are distinct.

For if not, let

$$x_i a = x_j a \quad \text{when} \quad i \neq j$$

$$\Rightarrow \quad x_i a - x_j a = 0 \quad \Rightarrow \quad (x_i - x_j)a = 0$$

$$\Rightarrow \quad x_i - x_j = 0$$

[$\because$ *$a \neq 0$ and D is without zero divisors*]

$$\Rightarrow \quad x_i = x_j,$$

whieh contradicts the given fact that all x_i are distinct.

$\therefore$ The produets

$$x_1 a, x_2 a, \ldots\ldots\ldots, x_n a$$

are all distinct.

Thus $x_1 a, x_2 a, \ldots\ldots\ldots, x_n a$ are n distinct elements for D in some other order.

Since D is an integral domain, therefore, it must contain unity.

Let $x_i a =$ for same value of $1 \leqslant i \leqslant n$.

In other words, for a given non-zero elemens a of D, there exists an element $b = x_i \in D$ such that $ab = 1$.

Thus b is the multiplicative inverse of a.

Thus multiplicative inverse of each non-zero element exists in D.

Hence D is a field.

Theorem II. *Every field F is an integral domain.*

Proof. Here we are to show that a field has no zero divisors.

Let $a, b \in F$ with $a \neq 0$ such that $ab = 0$.

Since $a \neq 0$, $\quad \therefore \quad a^{-1}$ exists.

Now $\quad ab = 0$

$$\Rightarrow \quad a^{-1}(ab) = a^{-1}0$$

$$\Rightarrow \quad (a^{-1}a)b = 0$$

$$\Rightarrow \quad b = 0.$$

Similarly $\quad ab = 0$ with $b \neq 0 \quad \Rightarrow \quad a = 0$

Thus F has no zero divisors.

Hence every field is an integral domain.

COMPARATIVE STUDY | Remember

Division Ring	Integral Domain	Field
1. It has at least two elements.	1. It has at least two elements.	1. It has at least two elements.
2. It is a ring with unity.	2. It is a ring with unity.	2. It is a ring with unity.
3. It is non-commutative ring.	3. It is a commutative ring.	3. It is a commutative ring.
4. It is a ring without zero divisors.	4. It is a ring without zero divisors.	4. It is a ring without zero divisors.
5. Cancellation laws hold.	5. Cancellation laws hold.	5. Concellation laws hold.
6. Every non-zero element has multiplicative inverse.		6. Every non-zero element has multiplicative inverse.
7. Set of non-zero elements form non-abelian multiplicative group.		7. Set of non-zero elements form abelian multiplicative group.

Conclusions.

(I) **Every field is an division ring but not vice-versa.**

(II) **Every field is an integral domain but not vice-versa.**

(III) **A field is a commutative division ring.**

Example 16. (*i*) *Give an example of a division ring which is not a field.*

(*ii*) *Give an example of an integral domain which is not a field.*

Sol. (*i*) The set of matrices

$$\begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}, \text{ where } a, b, c, d$$

are real numbers is a division ring which is not a field.

[$\because$ *Matrix multiplication is not, in general, commutative*]

(*ii*) The ring of integers is an integral domain which is not a field because all the elements do not have multiplicative inverses.

Example 17. *If p is a prime number, show that the ring of integers mod p is a field.* **(Important)** **[G.N.D.U. 1982]**

Sol. Please try yourself.

[**Hint.** Prove that Z_p has no zero divisor]

Example 18. *Show that the commutative ring D is an integral domain if and only if for a, b, $c \in D$, with $a \neq 0$ the relation*

$$ab = ac \quad \Rightarrow \quad b = c.$$ **(V. Important)**

Sol. Let D be an integral domain

i.e., D has no zero divisors.

We have :

$$ab = ac \quad \Rightarrow \quad ab - ac = 0$$

$$\Rightarrow \quad a(b-c) = 0 \quad \Rightarrow \quad b - c = 0$$

[$\because$ $a \neq 0$ *and D is without zero divisor*]

$$\Rightarrow \quad b = 0.$$

Conversely. Let $ab = ac \Rightarrow b = c$.

If possible, let $ab = 0$, where $a \neq 0$, $b \neq 0$.

Then we have $ab = a \,.\, 0$ [$\because$ $a \,.\, 0 = 0$]

$\Rightarrow$ $b = 0$. [*Left Cancellation Law*]

which is a contradiction.

Hence D is without zero divisor *i.e.,* D is an integral domain.

CHARACTERISTIC OF A RING

If 0 denotes the zero-element of a ring R and suppose there exists a positive integer n such that

$$na = a + a + \ldots\ldots + a = 0 \quad \forall a \in R$$

The smallest such positive integer n is called the characteristic of the ring R.

If such an integer n does not exist, the ring is said to have **characteristic zero or infinite.**

All the rings have characteristic zero.

The ring of integers modulus 6 has characteristic 6

since $\{1\} + \{1\} + \{1\} + \{1\} + \{1\} + \{1\} = \{6\} = \{0\}$.

Example 19. *Let a, b be commutative elements of a ring R of characteristic two. Show that*

$$(a+b)^2 = a^2 + b^2 = (a-b)^2.$$

Sol. We have : $ab = ba$ for $a, b \in R$.

Since characteristic of R is two, [*Given*]

$\therefore$ $x + x = 0 \quad \forall x \in R$

Now
$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= aa + ab + ba + bb\\ &= a^2 + ab + ba + b^2\\ &= a^2 + x + x + b^2 \qquad [\textit{Let } ab = ba = x]\\ &= a^2 + b^2.\end{aligned}$$

Similarly $(a-b)^2=(a-b)(a-b)$

$=a\,.\,a+a(-b)+(-b)a+(-b)(-b)$

$=a^2-ab-ba+b^2$

$=a^2-(ab+ba)+b^2$

$=a^2-(x+x)+b^2$ $[\because\ x+x=0]$

$=a^2+b^2.$

Example 20. *The characteristic of an integral domain is either zero or a prime number.* **(V. Important)**

Sol. Let D be an integral domain.

Let $a \in D$, where $a \neq 0$.

If $O(a)=0$, then characteristic of D is zero.

If $O(a)$ is finite, then characteristic of D is p.

To prove. *p is prime.*

Suppose that p is not prime.

Then $p=p_1p_2$, where $p_1 \neq 1$, $p_2 \neq 1$ and $p_1, p_2 < p$.

Since D is an integral domain, $\therefore$ $a \neq 0$

$\Rightarrow$ $aa \neq 0$ $\Rightarrow$ $a^2 \neq 0$

Now $O(a)=p$ $\Rightarrow$ $O(a^2)=p$

$\Rightarrow$ $pa^2=0$ $\Rightarrow$ $(p_1p_2)a^2=0$

$\Rightarrow$ $(a^2+a^2+\ldots\ldots$ *to* p_1p_2 terms$)=0$

$\Rightarrow$ $(p_1a)(p_2a)=0$

$\Rightarrow$ either $p_1a=0$ or $p_2a=0$

$[\because$ *D is without zero divisior*$]$

But $p_1 < p$ and $p_2 < p$.

Also p is the least positive integer such that $pa=0$.

Hence p is prime.

SUB-RINGS

Def *Let R be a ring. A non-empty sub-set S of the set R is said to be a sub-ring of R if it itself is a ring under the two induced operations.*

For Ex. (*I*) *Consider* $<I, +, .>$.

We know that I forms a ring under '+' and '.'

Consider $H_n = \{\ldots\ldots -2n, -n, 0, n, 2n, \ldots\ldots\}$

Clearly $H_n \subset R$.

Also $< H_n, +, . >$ is a ring.

Hence H_n is a subring of R.

(II) The set of integers is a sub-ring of the ring of rational numbers.

Remember. (I) If a ring is without zero divisors, then the sub-ring must also be without zero divisors.

(II) If a ring is commutative, then the sub-ring must also be commutative.

(III) If a ring is with unity, then the sub-ring may be without unity.

Theorem I. *The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring are*

(i) $a, b \in S \Rightarrow a-b \in S$

(ii) $a, b \in S \Rightarrow ab \in S$.

Proof. Necessary Conditions.

Let $<S, +, .>$ be a sub-ring of $<R, +, .>$

$\forall\, b \in S \Rightarrow -b \in S$ [$\because$ *S is a ring in itself*]

$\therefore\ \forall\, a \in S, -b \in S$

$\Rightarrow a+(-b) \in S$ [$\because$ *S is closed under addition*]

$\Rightarrow a-b \in S$.

Also $a, b \in S \Rightarrow ab \in S$

[$\because$ *S is closed under multiplication*]

Sufficient Conditions.

Given. $\forall\, a, b \in S \Rightarrow a-b \in S, ab \in S$

To prove. S is a ring.

Proof. Under Addition.

(i) **Associative Law.**

Since $S \subset R$ and associative law holds in R

$\therefore$ associative law also holds in S

(ii) **Existence of Identity**

$\forall\, a, a \in S \Rightarrow a-a \in S$

[$\because \forall\, a, b, \in S \Rightarrow a-b \in S$ *(given)*]

$\Rightarrow 0 \in S$

$\therefore$ The identity element $0 \in S$.

(iii) **Existence of Inverse.**

For $0, a \in S \Rightarrow 0-a \in S$

[$\because a, b \in S \Rightarrow a-b \in S$ *(given)*]

$\Rightarrow -a \in S$

$\therefore$ Inverse of every element of S exists.

(iv) **Closure Axiom.**

$\forall\, b \in S \Rightarrow -b \in S$ [*Inverse Property*]

$\therefore -a, b \in S \Rightarrow a-(-b) \in S$

[$\because a, b \in S \Rightarrow a-b \in S$ *(given)*]

$\Rightarrow a+b \in S$

$\therefore$ S is closed.

(*v*) **Commutative Law.**

Since $S \subset R$ and commutative law holds in R

$\therefore$ commutative law also holds in S.

Under Multiplication.

(*vi*) **Closure Axiom.**

$\forall\ a, b \in S \Rightarrow ab \in S$ [*Given*]

$\therefore$ S is closed.

(*vii*) **Associative Law.**

Since $S \subset R$ and associative laws holds in R

$\therefore$ associative law also holds in S.

(*viii*) **Distributive Laws.**

Since $S \subset R$ and distributive laws hold in R

$\therefore$ distributive laws also hold in S.

Hence S is a ring in itself.

Theorem II. *The intersection of two sub-rings is a sub-ring.*

Proof. Let S_1 and S_2 be two sub-rings of a ring R.

To prove. $S_1 \cap S_2$ is a sub-ring of R.

Since $0 \in S_1$ and $0 \in S_2$, $\therefore\ 0 \in S_1 \cap S_2$

$\therefore$ $S_1 \cap S_2$ is non-empty.

To show that $S_1 \cap S_2$ is a sub-ring, we have to prove that

$a \in S_1 \cap S_2, b \in S_1 \cap S_2 \Rightarrow a-b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$.

Now $a \in S_1 \cap S_2 \Rightarrow a \in S_1$ and $a \in S_2$

$b \in S_1 \cap S_2 \Rightarrow b \in S_1$ and $b \in S_2$.

Again $a \in S_1, b \in S_1 \Rightarrow a-b \in S_1$ and $ab \in S_1$ [$\because$ S_1 *is a sub-ring*]

and $a \in S_2, b \in S_2 \Rightarrow a-b \in S_2$ and $ab \in S_2$ [$\because$ S_2 *is a sub-ring*]

Now $a-b \in S_1, a-b \in S_2 \Rightarrow a-b \in S_1 \cap S_2$

and $ab \in S_1, ab \in S_2 \Rightarrow ab \in S_1 \cap S_2$

Thus $a \in S_1 \cap S_2, b \in S_1 \cap S_2 \Rightarrow a-b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$

Hence $S_1 \cap S_2$ is a sub-ring of R.

Generalisation. If $S_1, S_2, \ldots\ldots, S_n$ are sub-rings of a ring R,

then $\bigcap\limits_{i=1}^{n} S_i \ (= S_1 \cap S_2 \cap \ldots\ldots \cap S_n)$ is a sub-ring of R.

Note. *The union of two sub-rings may not be a sub-ring.*

For Ex. *Consider* $< Z, +, . >$

$$Z = \{\ldots\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$$
$$H_2 = \{\ldots\ldots -4, -2, 0, 2, 4, \ldots\ldots\ldots\ldots\}$$
$$H_3 = \{\ldots\ldots -6, -3, 0, 3, 6, \ldots\ldots\ldots\ldots\}$$

Clearly H_2 and H_3 are sub-rings of Z.

But $H_2 \cup H_3 = \{\ldots\ldots\ldots 0, 2, 3, 4, 6, \ldots\ldots\ldots\}$,
which is not a ring. [$\because$ *It is not closed under addition*]

Note. Let R be a ring.

Then {0} and R itself are **improper sub-rings** of R.

Other sub-rings, if any, are **proper sub-rings** of R.

Example 21. *Give an example of a ring with identity such that a sub-ring does not have an identity.*

Sol. The ring of even integers $\{\ldots\ldots -4, -2, 0, 2, 4, \ldots\ldots\}$ is a sub-ring without identity of the ring of integers $\{\ldots\ldots -2, -1, 0, 1, 2, \ldots\ldots\}$ with identity 1.

Example 22. *Prove that the sub-set S of all matrices of the form* $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ *with a, b, c integers, forms a sub-ring of the ring R of all* 2×2 *matrices having elements as integers.*

Sol. Let $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$
be any two elements of S.

Then $A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix} \in S$

[$\because$ *$a_1 - a_2$, $b_1 - b_2$, $c_1 - c_2$ are integers*]

and
$$AB = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$$
$$= \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix} \in S.$$

Thus $A \in S, B \in S \Rightarrow A - B \in S$ and $AB \in S$.

Hence S is a sub-ring of R.

Example 23. *Prove that the set S of all matrices of the form* $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ *with a and b integers, form a sub-ring of the ring R of all* 2×2 *matrices having elements as integers (rational or real).*

Sol. Please try yourself.

HOMOMORPHISMS

(a) Homomorphism.

Def *A mapping* φ *from the ring R into the ring R'*
φ : *R → R') is said to be homomorphism if*

(*i*) $\varphi(a+b)=\varphi(a)+\varphi(b)$

(*ii*) $\varphi(ab)=\varphi(a)\,\varphi(b) \quad \forall a, b \in R$.

(*b*) **Isomorphism.**

Def. *If the mapping φ is one-one, onto, then it called isomorphism.*

i.e. if $\varphi : R \to R'$

and φ is homomorphism and one-one,

then φ is called isomorphism.

Properties. *If φ is a homomorphism of R into R′, then*

(*i*) $\varphi(0)=0'$

(*ii*) $\varphi(-a)=-\varphi(a) \quad \forall \; a \in R$.

Proof. (*i*) We have $\varphi(a)+0'=\varphi(a)$ [∵ *0′ is identity of R′*]

$=\varphi(a+0)$ [∵ *a∈R and 0 is identity of R*]

$=\varphi(a)+\varphi(0)$ [∵ *φ is homomorphism*]

$\Rightarrow \quad 0'=\varphi(0)$ [*By Left Cancellation Law*]

Hence $\varphi(0)=0'$.

(*ii*) We have

$\varphi(a)+\varphi(-a)=\varphi(a+(-a))$ [∵ *φ is homomorphism*]

$=\varphi(0)$

$=0'$ [*By part (i)*]

∴ $\varphi(-a)$ is the additive inverse of $\varphi(a)$ in R′.

Hence $\varphi(-a)=-\varphi(a)$.

(*c*) **Kernal.**

Def. *If φ is a homomorphism of R into R′, then the kernal of φ, denoted by φ(I), is the set of all elements a∈R such that φ(a)=0′, the zero element of R′.*

Theorem. *If φ is a homomorphism of R into R′ with kernal φ(I), then*

(*i*) *φ(I) is a sub-group of R under addition.*

(*ii*) *If a∈φ(I) and r∈R, then both ar and ra are in φ(I)*

Proof. (*i*) Let $a, b \in \varphi(I)$,

then $\varphi(a)=0', \quad \varphi(b)=0'$ [*Def. of Kernal*]

Now $\varphi(a+(-b))=\varphi(a)+\varphi(-b)$ [∵ *φ is homomorphism*]

$=\varphi(a)-\varphi(b)$

$=0'-0'$

$=0'$

$\Rightarrow \quad a+(-b) \in \varphi(I)$.

Hence $\varphi(I)$ is a sub-group of R under addition.

(*ii*) Suppose $a \in \varphi(I)$, $r \in R$,

then $\varphi(a)=0'$. [*Def. of Kernal*]

Now $\varphi(ar)=\varphi(a)\,.\,\varphi(r)$ [$\because$ φ *is homomorphism*]

$$=0'\,.\,\varphi(r)$$

$$=0'$$

$\Rightarrow$ $ar \in \varphi(I)$

Similarly $ra \in \varphi(I)$.

Example 24. *$R=R_1=\{a+b\sqrt{3}/a, b \in I\}$ with addition and multiplication of real numbers be a ring. Then prove that*

$f_1 : R \to R_1$ defined by $f_1(a+b\sqrt{3})=a-b\sqrt{3}$

is a homomorphism. **(Important)** [G.N.D.U. 1976]

Sol. $\varphi(a_1+b_1\sqrt{3}+a_2+b_2\sqrt{3})$

$$=\varphi[(a_1+c_2)+(b_1+b_2)\sqrt{3}]$$

$$=(a_1+a_2)-(b_1+b_2)\sqrt{3}$$

$$=(a_1-b_1\sqrt{3})+(a_2-b_2\sqrt{3})$$

$$=\varphi(a_1+b_1\sqrt{3})+\varphi(a_2+b_2\sqrt{3})$$

Also $\varphi[(a_1+b_1\sqrt{3})\,.\,(a_2+b_2\sqrt{3})]$

$$=\varphi[(a_1a_2+3b_1b_2)+(a_1b_2+b_1a_2)\sqrt{3}]$$

$$=(a_1a_2+3b_1b_2)-(a_1b_2-b_1a_2)\sqrt{3}$$

$$=(a_1-b_1\sqrt{3})(a_2-b_2\sqrt{3})$$

$$=\varphi(a_1+b_1\sqrt{3})\,.\,\varphi(a_2+b_2\sqrt{3}).$$

Hence φ is a homomorphism.

IDEALS AND QUOTIENT RINGS

(*a*) Two-Sided Ideal

Def. *A non-empty sub-set U of a ring R is said to be* (*two-sided*) *ideal of R if*

(*i*) *U is a sub-group of R under addition*

(*ii*) $\forall$ *$u \in U$ and $r \in R$, both ur and ru are in U.*

(*b*) Left Ideal

Def. *A non-empty sub-set S of a ring R is said to be left ideal of R if*

(*i*) *S is a sub-group of R under addition*

(*ii*) $\forall$ $s \in S$ *and* $r \in R$, $sr \in S$.

(*c*) Right Ideal

Def. *A non-empty sub-set S of a ring R is said to be right ideal of R if*

(*i*) *S is a sub-group of R under addition*

(*ii*) $\forall$ $s \in S$ *and* $r \in R$, $sr \in S$.

$\Rightarrow \quad U+a'b'=U+ab \quad [\because \; a'b'-ab \in U]$

$\Rightarrow \quad (U+a')(U+b')=(U+a)(U+b).$

Thus multiplication composition is well-defined.

Hence both the compositions are well-defined.

To prove. *R/U is a ring.*

Under Addition :

(*i*) **Closure Axiom.**

$\forall \; U+a, U+b \in R/U$, where $a, b \in R$

$(U+a)+(U+b)=U+(a+b)$

Now $\because a, b \in R \Rightarrow a+b \in R \quad [\because \; R \text{ is a ring}]$

$\therefore \quad (U+a)+(U+b) \in R/U.$

(*ii*) **Associative Law.**

$\forall \; U+a, U+b, U+c \in R/U,$

where $a, b, c \in R$

$$(U+a)+[(U+b)+(U+c)]=(U+a)+[U+(b+c)]$$
$$=U+[a+(b+c)]=U+[(a+b)+c]$$
$[\because \; a, b, c \in R$ *and R is a ring*$]$
$$=[U+(a+b)]+(U+c)$$
$$=[(U+a)+(U+b)]+(U+c)$$

$\therefore$ Associative Law holds.

(*iii*) **Existence of Identity.**

U works for identity of R/U

because $(U+a)+U=U+a=U+(U+a).$

(*iv*) **Existence of Inverse.**

$U-a$ works as inverse of $U+a$

because $(U+a)+(U-a)=U+a+(-a)$
$$=U+0=U$$

and $(U-a)+(U+a)=U+(-a)+a$
$$=U+0=U.$$

(*v*) **Commutative Law.**

$\forall \; U+a, U+b \in R/U$, where $a, b \in R$

$$(U+a)+(U+b)=U+(a+b)$$
$$=U+(b+a)$$
$[\because \; a, b \in R$ *and R is a ring*$]$
$$=(U+b)+(U+a).$$

Under Multiplication :

(*vi*) **Closure Axiom.**

$\forall \; U+a, U+b \in R/U$, where $a, b \in R$

$$(U+a)(U+b)=U+ab$$

Now $\because \quad a, b \in R \Rightarrow ab \in R$ [$\because$ *R is a ring*]

$\therefore \quad (U+a)(U+b) \in R/U.$

(vii) Associative Law.

$\forall\ U+a,\ U+b,\ U+c \in R/U$, where $a, b, c \in R$

$$(U+a) \cdot [(U+b)(U+c)] = [(U+a)(U+bc)]$$
$$= U+[a(bc)] = U+[(ab)c]$$

[$\because$ *$a, b, c \in R$ and R is a ring*]

$$= [U+ab](U+c)$$
$$= [(U+a)(U+b)](U+c)$$

$\therefore$ Associative Law holds.

(viii) Distributive Laws.

$$(U+a) \cdot [(U+b)+(U+c)]$$
$$= (U+a) \cdot [U+(b+c)] = U+a(b+c)$$
$$= U+(ab+ac)$$
$$= (U+ab)+(U+ac)$$
$$= (U+a) \cdot (U+b)+(U+a) \cdot (U+c)$$

Similarly $[(U+b)+(U+c)] \cdot (U+a)$

$$= (U+b) \cdot (U+a)+(U+c) \cdot (U+a)$$

Hence R/U forms a ring.

Homomorphism.

Let $\varphi : R \to R/U$ defined by

$$\varphi(a) = a+U \qquad \forall\ a \in R.$$

$$\therefore \quad \varphi(a+b) = a+b+U = (a+U)+(b+U)$$
$$= \varphi(a)+\varphi(b)$$

and
$$\varphi(ab) = ab+U = (a+U) \cdot (b+U)$$
$$= \varphi(a) \cdot \varphi(b)$$

Hence φ is a homomorphism.

R/U is called the **quotient ring** or **factor ring** or **difference ring** or **residue class ring** where U is an ideal of R.

Cor. 1. *If R is a ring with unity, then R/U is also with unity.*

Proof. Since R is a ring with unity,

$\therefore \quad \exists\ 1 \in R$ s.t. $\quad a \cdot 1 = 1 \cdot a = a \quad \forall\ a \in R$ ...(1)

Since $1 \in R$, $\quad \therefore \quad U+1 \in R/U$.

$U+1$ works as unity of R/U.

Because $(U+a)(U+1) = U+a \cdot 1 = U+a$.

Hence R/U is with unity.

Cor. 2 *If R is an abelian ring, then R/U is also an abelian ring.*

Proof $\forall\ U+a,\ U+b \in R/U$, where $a, b \in R$.

To prove. $(U+a)+(U+b)=(U+b)(U+a)$

$$(U+a)+(U+b)=U+ab$$
$$=U+ba \qquad [\because\ R \text{ is a ring}]$$
$$=(U+b)(U+a).$$

Hence R/U is commutative.

Example 25. (*i*) *Prove that the intersection of two left ideals of a ring is again a left ideal of the ring.*

(*ii*) *Prove that the intersection of two right ideals of a ring is again a right ideal of the ring.*

Sol. (*i*) Let I_1 and I_2 be two left ideals of the ring R.

Then I_1 and I_2 are sub-groups of R under addition

$\Rightarrow$ $I_1 \cap I_2$ is also a sub-group of R under addition.

Now $s \in I_1 \cap I_2 \Rightarrow s_1 \in I_1,\ s \in I_2$.

Since I_1 is a left ideal of R,

$\therefore$ $r \in R,\ s \in I_1 \Rightarrow rs \in I_1$

Since I_2 is a left ideal of R,

$\therefore$ $r \in R,\ s \in I_2 \Rightarrow rs \in I_2$.

Now $rs \in I_1,\ rs \in I_2 \Rightarrow rs \in I_1 \cap I_2$

$\Rightarrow$ $I_1 \cap I_2$ is a left ideal of R.

Hence the result.

(*ii*) Please try yourself.

Example 26. *The set N of all 2×2 matrices of the form*

$$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$$

for a, b integers is a left ideal but not a right ideal in the ring R of all 2×2 matrices with elements as integers. **(Important)**

Sol. Let $A=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix},\ B=\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$

be any two elements of the set N, where a, b, c, d are integers.

Then $$A-B=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}-\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$$
$$=\begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in N$$

because $a-c$ and $b-d$ are also integers.

Also $$AB=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$$
$$=\begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix}\in N$$

Thus N is a sub-group of R under addition.

Let $u=\begin{bmatrix} x & y \\ z & t \end{bmatrix}$ be an element of R.

We have $$A=\begin{bmatrix} x & y \\ z & t \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$$
$$=\begin{bmatrix} xa+yb & 0 \\ za+tb & 0 \end{bmatrix}\in N$$

because $xa+yb$ and $za+tb$ are integers.

Thus N is a left ideal of R.

Also we have

$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\in N \quad \text{and} \quad \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\in R$$

yet $$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}=\begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}\notin N$$

Thus N is not a right ideal.

Hence the result.

Example 27. *Let M be the ring of 2×2 matrices lver integers Then show that $K=\left\{\begin{bmatrix} a & b \\ o & o \end{bmatrix} \middle/ a, b\in Z\right\}$ is a right idea of M but not a left ideal of K.*

[G.N.D.U. 1980 S, 77]

Sol. Please try yourself.

Example 28. *If R is a ring and $a\in R$, let $M=\{x\in R/ax=0\}$. Prove that M is a right ideal of R.*

Sol. Since $0\in R$ such that $a0=0$,

$\therefore$ M is *non-empty.*

Let x_1, x_2 be any two elements of M.

Then $\quad ax_1=0, \quad ax_2=0$

$\therefore \quad a(x_1-x_2)=ax_1-ax_2=0-0=0$

$\Rightarrow \quad x_1-x_2\in M$

$\therefore$ *M is a sub-group of R under addition.*

Let $x\in M$, $y\in R$.

To prove. $xy\in M$

$x\in M \quad \Rightarrow \quad ax=0 \qquad$ [*Def.*]

$\Rightarrow$ each non-zero element of R possesses multiplicative inverse.

Hence R is a field.

Example 32. *If U is an ideal of R and $1 \in U$, prove that $U = R$.*

Sol. Let x be any element of R.

Now $1 \in U, x \in R \Rightarrow 1 . x \in U \Rightarrow x \in U$.

Thus every element of R is in U.

$\therefore$ $\quad R \subseteq U \quad$ ...(1)

But $\quad U \subseteq R \quad$ ...(2)

Combining (1) and (2),

$$U = R, \text{ which is true.}$$

Example 33. *If A and B are ideals of R, let*

$$A+B=\{u+v \mid u \in U, v \in V\}.$$

Prove that $A+B$ is also an ideal of R. [G.N.D.U. 1980 S]

Sol. Let u_1+v_1 and u_2+v_2 belong to A+B,

where $u_1, u_2 \in A$ and $v_1, v_2 \in B$.

Since A is an ideal of R,

$\therefore$ A is a sub-group of R under addition.

Since B is an ideal of R,

$\therefore$ B is a sub-group of R under addition.

Now $u_1, u_2 \in A \Rightarrow u_1 - u_2 \in A$

and $v_1, v_2 \in B \Rightarrow v_1 - v_2 \in B$

$\therefore$ $(u_1+v_1)-(u_2+v_2)=(u_1-u_2)+(v_1-v_2) \in A+B$.

$\therefore$ A+B is a sub-group of R under addition.

Now let $r \in R$ and $u_1+v_1 \in A+B$

Thus $u_1 \in A$, $v_1 \in B$, we have

$$r(u_1+v_1)=ru_1+rv_1 \in A+B$$

[$\because$ *A and B are ideals,* $\therefore$ $ru_1 \in A$ *and* $rv_1 \in B$]

Similarly $(u_1+v_1)r=u_1r+v_1r \in A+B$.

Hence A+B is also an ideal of R.

Example 34. *If U is a left ideal of a ring R and let*

$$\lambda(U)=\{x \in R / xu=0 \ \forall \ u \in U\}.$$

Prove that $\lambda(U)$ is a two-sided ideal of R. **[Important]**

Sol. Since $0 \in R$ such that $0u=0 \ \forall \ u \in U$.

$\therefore$ *$\lambda(U)$ is non-empty.*

Let x_1 and x_2 be any two elements of $\lambda(U)$.

Then $x_1u=0$ and $x_2u=0 \quad \forall \quad u \in U$

Now $(x_1-x_2)u=x_1u-x_2u=0-0=0 \quad \forall \; u \in U$

$\Rightarrow \quad x_1-x_2 \in \lambda(U)$.

Let x be any element of $\lambda(U)$ and r any element of R.

Then $xu=0 \quad \forall \quad u \in U$ [*Def.*]

$\Rightarrow \quad r(xu)=r0 \quad \forall \quad u \in U$

$\Rightarrow \quad (rx)u=0 \quad \forall \quad u \in U$

$\Rightarrow \quad rx \in \lambda(U)$.

Also U is a left ideal of R [*Given*]

$\therefore \quad ru \in U \quad \forall u \in U$

Since $x \in \lambda(U)$,

$\therefore \; x \in \lambda(U),\, ru \in U \quad \Rightarrow \quad x(ru)=0 \;\forall\; u \in U$

$\Rightarrow \quad (xr)u=0 \;\forall\; u \in U$

$\Rightarrow \quad xr \in \lambda(U)$

Thus $x \in \lambda(U),\, r \in R \quad \Rightarrow \quad xr \in \lambda(U)$

and $\quad rx \in \lambda(U)$.

Hence $\lambda(U)$ is a two-sided ideal of R.

Example 35. *If F is a field, prove that {0} and F itself are only its ideals.* *Or*

Prove that a field has no proper ideals.

Sol. Let I be any non-zero ideal of F.

Let $a(\neq 0) \in I$. Then $a^{-1} \in F$

Since I is an ideal,

$\therefore \quad a \in I,\, a^{-1} \in F \;\Rightarrow\; aa^{-1} \in I \;\Rightarrow\; 1 \in I$

Let x be any element of F.

Then $1 \in I,\; x \in F \;\Rightarrow\; 1 . x \in I \;\Rightarrow\; x \in I$.

Thus every element of F is in I.

$\therefore \quad F \subseteq I$ ...(1)

Also $\quad I \subseteq F$ ...(2)

Combining (1) and (2), $I=F$.

Hence the only ideals of F are {0} and F itself.

Example 36. *If U and V are two ideals of the ring R. Let UV be the set of all those elements of R which can be written as finite sums of elements of the form uv, where $u \in U$ and $v \in V$. Prove that UV is also an ideal of R.* **(V. Important)**

Sol. Here U and V are two ideals of the ring R.

Let $UV=\{u_1v_1+u_2v_2+\ldots\ldots+u_nv_n/u_1, u_2, \ldots\ldots, u_n \in U,$
$v_1, v_2, \ldots\ldots, v_n \in V$, n being a +ve integer$\}$.

when $x-y \in A$, then $y=x-(x-y) \in A$.

But $y \notin A$, which leads to contradiction.

Again when $x-y \in B$, then $x=(x-y)+y \in B$.

But $x \notin B$, which leads to contradiction.

Thus our supposition is wrong.

Hence $A \subseteq B$ and $B \subseteq A$.

PRIME AND MAXIMAL IDEALS

Definitions

(*a*) **Prime Ideal.** *Let R be a commutative ring. An ideal of R is said to be prime ideal of R iff* $ab \in P \Rightarrow$ *either* $a \in P$ *or* $b \in P$. [G.N.D.U. 1981]

For Example. *Consider the ring* $<Z, +, .>$.

Let the set of multiples of 15 be

$$H_{15} = \{\ldots\ldots -15, 0, 15, \ldots\ldots\}$$

Here H_{15} is an ideal of I [*Verify* !]

Also $15 \in H_{15}$ *i.e.* $3 \cdot 5 \in H_{15}$, where $3 \cdot 5 \in I$

But neither $3 \in H_{15}$ nor $5 \in H_{15}$.

Hence H_{15} is not a prime ideal.

(*b*) **Maximal Ideal.** *Let R be a ring. An ideal M af R is said to be maximal ideal iff there exists no ideal of R containing M i.e. if N is an ideal of R containing M, then either N=M or N=R.* [G.N.D.U. 1981, 80 S]

Thus the ideal M of a ring R is maximal if there exists no ideal between M and R.

For Example. The ideal of the ring of integers generated by a prime number is a maximal ideal.

e.g. $(5) = \{\ldots\ldots -10, -5, 0, 5, 10, \ldots\ldots\}$

and $(7) = \{\ldots\ldots -14, -7, 0, 7, 14, \ldots\ldots\}$ are maximal ideals.

(*c*) **Principal Ideal.** *An ideal generated by a single element is called a principal ideal.*

(*d*) **Principal Ideal Ring.** *The commutative ring where every ideal is principal is said to be principal ideal ring.*

Theorem 1. *Prove that if P is an ideal of a commutative ring R, then P is a prime ideal of R iff R/P is an integral domain.* [G.N.D.U. 1977]

Proof. $R/P = \{P+b \ \forall \ b \in R\}$.

Let R/P be an I.D. *i.e.* it is without zero divisor.

To Prove. P is prime ideal

Let $P+b=\bar{b}$ and $P+c=\bar{c}$, $P+1=\bar{1}$, $P+0=\bar{0}$.

$\forall \ b, c \in R$, let $bc \in P$.

To prove. Either $b \in P$ or $c \in P$

$$P+bc=P \qquad [\because bc \in P]$$

$$\Rightarrow \quad (P+b)(P+c)=P$$

$$\Rightarrow \quad \bar{b}\,\bar{c}=\bar{0}$$

$$\Rightarrow \quad \text{either} \quad \bar{b}=\bar{0} \quad \text{or} \quad \bar{c}=\bar{0}$$

Case I. When $\bar{b}=\bar{0}$.

Then $\quad P+b=P \quad \Rightarrow \quad b \in P.$

Case II. When $\bar{c}=\bar{0}$.

Then $\quad P+c=P \quad \Rightarrow \quad c \in P.$

Hence P is a prime ideal.

Conversely. Let P be a prime ideal.

To prove. R/P is an integral domain.

$$\forall\ \bar{b}, \bar{c} \in R/P, \text{ if possible let } \bar{b}\,\bar{c}=\bar{0}$$

$$\Rightarrow \quad (P+b)(P+c)=P$$

$$\Rightarrow \quad P+bc=P \quad \Rightarrow \quad bc \in P$$

$$\Rightarrow \quad \text{either} \quad b \in P \quad \text{or} \quad c \in P \qquad [\because P \text{ is a prime ideal}]$$

$$\Rightarrow \quad \text{either } P+b=P \quad \text{or} \quad P+c=P$$

$$\Rightarrow \quad \text{either} \quad \bar{b}=\bar{0} \quad \text{or} \quad \bar{c}=\bar{0},$$

which is a contradiction. $\qquad [\because \textit{neither } \bar{b}\neq 0 \textit{ nor } \bar{c}=\bar{0}]$

$$\therefore \quad \bar{b}\,\bar{c}\neq\bar{0}.$$

Hence R/P is an integral domain.

Theorem II. *If R is a commutative ring with unit element and M is an ideal of R, then M is a maximal ideal of R iff the residue class ring R/M is a field.* **[V. Important]**

[G.N.D.U. 1982, 81, 80 S]

Proof. R is a commutative ring with unit element

$\Rightarrow$ R/M is also a commutative ring with unit element.

Let R/M be a field.

To prove. M is a maximal ideal of R.

If possible, let N be any ideal of R containing M properly

i.e. $\quad \exists\ n \in N$ such that $n \notin M$ ...(1)

To prove. $N=R$ *i.e.* $N \subseteq R$ and $R \subseteq N$.

Since N is an ideal of R,

$$N \subseteq R \qquad ...(2)$$

$\therefore \quad n \in M + nR$

and $\quad n \in N$ such that $n \notin M$

$\therefore \quad M + nR \supsetneq M$ properly

$\Rightarrow \quad M + nR = R \qquad$ [$\because$ *M is maximal ideal of R*]

Since $\quad 1 \in R \qquad$ [$\because$ *R is a ring with unit element*]

$\therefore \quad 1 \in M + nR$

$\therefore$ 1 can be expressed as

$$1 = m + nr \qquad \forall\, m \in M,\ \forall\, r \in R$$

$$\Rightarrow \quad -m = nr - 1 \qquad \ldots(5)$$

Now $\quad m \in M \Rightarrow -m \in M \quad$ [$\because$ *M is an ideal of R*]

$\Rightarrow \quad nr - 1 \in M \qquad$ [*Using* (5)]

$\Rightarrow \quad M + nr - 1 = M \qquad$ [$\because$ $H + h = H$]

$\Rightarrow \quad M + nr = M + 1$

$\Rightarrow \quad (M + n)(M + r) = M + 1$

$\Rightarrow \quad \bar{n}\,\bar{r} = 1$

$\Rightarrow \quad \bar{r}$ is the inverse of $\bar{n}$ and $\bar{r} \in R/M$.

Thus inverse of each non-zero element exists in R/M.

Hence R/M is a field.

Theorem III. *Every maximal ideal in a commutative ring R with unity is a prime ideal.* [G.N.D.U. 1980 S]

Proof. Let M be a maximal ideal of R

$\Rightarrow$ R/M is a field [*Theorem II*]

$\Rightarrow$ R/M is an integral domain

[$\because$ *Every field is an integral domain*]

$\Rightarrow$ M is prime ideal. [*Theorem I*]

Hence the result.

Remember. If R is a commutative ring with unity,

then (*i*) **An ideal M of R is maximal iff R/M is a field**

(*ii*) **An ideal P of R is prime iff R/P is an integral domain**

(*iii*) **Every maximal ideal of R is a prime ideal.**

Example 38. *Find the prime and maximal ideals of* Z_{12}.

Sol. $Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Let $\quad P_1 = \{0, 2, 4, 6, 8, 10\}$, $P_2 = \{0, 3, 6, 9\}$,

$P_3 = \{0, 4, 8\}$, $P_4 = \{0, 6\}$.

(*i*) P_1 and P_2 are only prime ideals.

P_3 and P_4 are not prime ideals.

[$\because$ $4 \in P_3$ but neither $2 \in P_3$ nor $2 \in P_3$]

(*ii*) P_1 and P_2 are maximal ideals.

[$\because$ *There is no ideal which is greater than P_1 and P_2*]

P_3 and P_4 are not maximal ideals.

Example 39. *Let Z be a ring of integers and let $P=\{6z/z \in Z\}$. Prove that P is an ideal of Z.*

Is P a maximal ideal.

Sol. $Z=\{\ldots\ldots\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$

and $P=\{\ldots\ldots\ldots -12, -6, 0, 6, 12, \ldots\ldots\ldots\ldots\}$

(*i*) Clearly P is an abelian group under addition. [*Verify* !]

Let $6y \in P$, $z \in Z \Rightarrow (6y)z=6(yz) \in P$.

Hence P is an ideal of Z.

[$\because$ *$y, z \in Z \Rightarrow yz \in Z$ because Z is a ring*]

(*ii*) P is not a maximal ideal of Z,

because there is an ideal $P'=\{\ldots\ldots -6, -3, 0, 3, 6, \ldots\ldots\}$, which contains P properly.

Example 40. *Let R be the ring of all real—valued continuous functions defined on [0, 1]. Let $M=\{f(x) \in R\ ;\ f(\frac{1}{3})=0\}$. Show that M is a maximal ideal of R.* **(V. Important)** [G.N.D.U. 1982]

Sol. The function $w : R \to R$ given by

$w(x)=0\ \forall\ x \in R$ belongs to M.

Thus M is non-empty.

Let $f, g \in M$.

Then $(f-g)(\frac{1}{3})=f(\frac{1}{3})-g(\frac{1}{3})=0 \Rightarrow f-g \in M$.

Let $f \in M$, $h \in R$,

then $hf(\frac{1}{3})=h(\frac{1}{3})f(\frac{1}{3})=0 \Rightarrow hf \in M$
$\Rightarrow fh \in M$

[$\because$ *R is commutative*]

Thus M is an ideal of R.

Clearly $M \neq R$ [$\because$ *$x \in R$ given by $\theta(x)=1 \notin M$*]

Let N be an ideal of R such that $M<N$.

$\exists\ \lambda \in N, \lambda \notin M \Rightarrow \lambda(\frac{1}{3}) \neq 0$ *i.e.* let $\lambda(\frac{1}{3})=c$, where $c \neq 0$.

Consider $\mu \in R$ given by $\mu=\lambda-\beta$, where $\beta(x)=c\ \ \forall\ x \in [0, 1]$

Then $\mu(\frac{1}{2})=\lambda(\frac{1}{2})-\beta(\frac{1}{2})$

$=c-c=0$

$\Rightarrow \quad \mu\in M \Rightarrow \mu\in N.$

$\therefore \quad \beta=\lambda-\mu\in N.$

Let us define $\gamma\in R$ by $\gamma(x)=\frac{1}{c}\ \forall\ x\in[0, 1]$

Then $\forall\ x\in[0, 1], \gamma\beta(x)=\gamma(x)\beta(x)=1=\theta(x)$

$\Rightarrow \quad \gamma\beta=\theta\in N$

$\Rightarrow \quad N=R.$ [$\because$ *θ is unity of R*]

Hence M is a maximal ideal of R.

QUOTIENT FIELD OF AN INTEGRAL DOMAIN

Def. *A field K is said to be a quotient field of an integral domain D if K contains D and is itself contained in every field containing D.*

For Example. The field Q of rational numbers is the quotient field of the integral domain I of integers.

Def. *A ring R is imbedded in a ring R′ if there exists an isomorphism of R into R′.*

R′ is said to be **an extension of R** or **an over ring of P** if R is imbedded in R′.

Theorem. *Every integral domain can be imbedded in a field.* **(V. Important)** [Pbi. U. 1978]

Or

If I is an integral domain, then it is possible to construct a quotient field from the elements of the integral domain. The quotient field contains a sub-system D which is isomorphic to I.

Proof. Consider the set of ordered pairs (a, b) such that $a\in I$ and $b\in I'$, where I′ is the set of non-zero elements of **I**. Let us define a relation

$$(a, b) \sim (c, d) \text{ if } ad=bc.$$

To prove. It is an equivalence relation.

(*i*) **Reflexive.** $(a, b) \sim (a, b)$.

Proof. $(a, b) \sim (a, b)$

if $ab = ba$, which is true.

[$\because$ *R is a commutative ring*]

(*ii*) **Symmetric.** $(a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$.

Proof. $(a, b) \sim (c, d) \Rightarrow ad=bc$

$\Rightarrow \quad da=cb$ [$\because$ *R is a commutative ring*]

$\Rightarrow \quad cb=da$

$\Rightarrow \quad (c, d) \sim (a, b).$

(*iii*) **Transitive.** $(a, b) \sim (c, d)$; $(c, d) \sim (e, f)$

$\Rightarrow (a, b) \sim (e, f)$

Proof. $(a, b) \sim (c, d) \Rightarrow ad=bc$ ...(1)

$(c, d) \sim (e, f) \Rightarrow cf=de$ ...(2)

Multiplying (1) by f, $fad=fbc$ ...(3)

Multiplying (2) by b, $bcf=bde$ ...(4)

From (2) and (4), $fad=bde$ [$\because$ *R is a commutative ring*]

$\Rightarrow \quad fad=bed$ [$\because$ *R is a commutative ring*]

$\Rightarrow \quad fa=be$ [*Cancellation Law holds*]

$\Rightarrow \quad af=be$ [$\because$ *R is a commutative ring*]

$\Rightarrow \quad (a, b) \sim (e, f).$

Thus the relation is an equivalence.

The equivalence relation will decompose $I \times I'$ into equivalent disjoint classes.

Let the class of all pairs equivalent to (a, b) be denoted by a/b and we define the sum and product as below :

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d}=\frac{ac}{bd}.$$

This set of equivalence classes with two compositions (defined above) forms a field.

The zero element of the field is $\frac{0}{b}$.

The additive inverse of $\frac{a}{b}$ is $\frac{-a}{b}$.

The unity element is $\frac{1}{1}$, where 1 is the unity of I.

The multiplicative inverse of $\frac{a}{b}$ $(a \neq 0)$ is $\frac{b}{a}$

$$\left[\because \frac{a}{b} \cdot \frac{b}{a}=1\right]$$

Thus the field is the required quotient field of the integral domain I.

To prove. There exists a sub-set of this field which is isomorphic to I, the integral domain.

Let us denote the sub-set of the field which contains classes

$$\frac{a}{1}, \frac{b}{1}, \frac{c}{1}, \ldots\ldots\ldots$$

by D.

Let us define $\varphi : D \rightarrow I$ such that

$$\varphi\left(\frac{a}{1}\right)=a, \text{ where } \frac{a}{1} \in D \text{ and } a \in I.$$

The mapping φ is one-one.

$$\left[\because \varphi\left(\frac{a}{1}\right)=\varphi\left(\frac{b}{1}\right) \Rightarrow a=b \right]$$

The mapping φ is onto.

Also $\varphi\left(\frac{a}{1}+\frac{b}{1}\right)=\varphi\left(\frac{a+b}{1}\right)=a+b=\varphi\left(\frac{a}{1}\right)+\varphi\left(\frac{b}{1}\right)$.

and $$\varphi\left(\frac{a}{1}\cdot\frac{b}{1}\right)=\varphi\left(\frac{ab}{1}\right)=ab=\varphi\left(\frac{a}{1}\right)\varphi\left(\frac{b}{1}\right).$$

Hence $\quad D \cong I.$

4

Polynomial Rings

[*Not meant for G.N.D.U. Students*]

DEFINITIONS

(*a*) **Polynomial.** Let R be a ring. Let $x \notin R$, where x is called **indeterminate**.

The expression of the form

$$f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots\dots\dots + a_nx^n,$$

$\forall\ a_i \in R$ *and n is a non-negative integer, is called the polynomial in x over R.*

Here a_ix^i are called the **terms** of the polynomial and a_i are called the **co-efficients** of the terms of the polynomial.

For Example. (*i*) *Consider* $5x^0 - 7x^2 - 8x^4 - \frac{3}{2}x^5$.

This is called a polynomial in x.

Since the co-efficients are rationals, therefore, it is a polynomial in x over the field of rationals.

(*ii*) *Consider* $5x^2 + \pi x^3 + 7x^4$.

This is a polynomial over the field of reals.

(*b*) **Monic Polynomial.** *A polynomial is called monic when the leading co-efficient is the unity element of F.*

(*c*) **Equal Polynomials.**

Let $\quad f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots\dots + a_ix^i + \dots\dots + a_mx^m$

and $\quad g(x) = b_0x^0 + b_1x^1 + b_2x^2 + \dots\dots + b_ix^i + \dots\dots + b_nx^n$

be two polynomials over R.

$f(x) = g(x)$ iff co-efficients of x are same on both sides except zero co-efficients.

i.e., $f(x) = g(x)$ iff $a_i = b_i\ \forall\ i > 0$ except zero co-efficients.

For Example. $5x^0 + 7x^3 + 9x^7$ is a polynomial over integers.

$\therefore$ It is a polynomial in x over the ring of integers.

Again $\quad 5x^0 + 0.x^1 + 0.x^2 + 7x^3 + 0.x^4 + 0.x^5 + 0.x^6 + 9x^7 \quad \dots(2)$

These polynomials are equal.

[$\because$ *Co-effs. of like powers of x on both sides are equal*]

(*d*) **Ring of Polynomials**

Let F be a field. By the ring of polynomials in x, written as F[x], we mean the set of all symbols.

$$a_0x^0+a_1x^1+a_2x^2+\ldots\ldots+a_nx^n,$$

where n is a non-negative integer and whose co-efficients

$$a_0, a_1, a_2, \ \ldots, a_n \text{ all} \in \text{F}.$$

Thus $\quad R[x]=\{f(x)/f(x)=a_0x^0+a_1x^1+a_2x^2+\ldots\ldots+a_nx^n\}$,

where $a_i \in R$ and n is non-negative integer.

(*e*) **Operations on polynomials.**

Let $\quad f(x)=a_0x^0+a_1x^1+\ldots\ldots+a_ix^i+\ldots\ldots+a_mx^m$

and $\quad g(x)=b_0x^0+b_1x^1+\ldots\ldots+b_ix^i+\ldots\ldots+b_nx^n$,

(*i*) $\quad$ **Sum** $=f(x)+g(x)=b_0x^0+c_1x^1+\ldots\ldots+c_ix^i+\ldots+c_tx^t$,

where for each i, $\; c_i=a_i+b_i$.

For Example. To add $1+x$ and $2+3x+x^2$, we consider $1+x$ as $1+x+0x^2$ and add to get $3+4x+x^2$.

(*ii*) Product $f(x)g(x)=c_0x^0+c_1x^1+\ldots\ldots+c_kx^k$,

where $\quad c_t=a_tb_0+a_{t-1}b_1+a_{t-2}b_2+\ldots\,.+a_0b_t$

For Example. $(1+x+x^2)(2-x^2+x^3)=c_0+c_1x+c_2x^2+\ldots\ldots$

$$=2+2x+x^2+x.^5$$

(*f*) **Degree of a polynomial.**

Let $\quad f(x)=a_0x^0+a_1x^1+\ldots\ldots+a_nx^n$, where $a_n\neq 0$ be a polynomial in x.

Then the degree of $f(x)$, written as deg $f(x)=n$.

Thus the highest power of x in the polynomial is called itr degree.

Note. The degree of a polynomial is always non-negative.

(*i*) *The degree of a zero polynomial is undefined.*

Thus the polynomial $0x^0+0x^1+0x^2+\ \ldots$ has no degree.

(*ii*) *The degree of a constant polynomial is zero.*

Thus the polynomial a_0x^0 has zero degree.

(*iii*) **Degree of the Sum.**

Let $f(x)$ be a polynomial of degree m

and $\quad g(x)$ be a polynomial of degree n.

Then (I) deg $[f(x)+g(x)]=\max.\ (m, n)$ when $m\neq n$

(II) deg $[f(x)+g(x)]\leqslant m$ $\quad$ when $m=n$,

provided $f(x)+g(x)$ is not a zero polynomial.

(*iv*) **Degree of the product.**

If $f(x)$ and $g(x)$ are two non-zero elements of F[x], then

$$\deg\,[f(x)g(x)]=\deg\, f(x)+\deg\, g(x)].$$

Proof. Let $f(x)=a_0x^0+a_1x^1+a_2x^2+......+a_mx^m \quad (a_m\neq 0)$

and $g(x)=b_0x^0+b_1x^1+b_2x^2+......+b_nx^n \quad (b_n\neq 0)$

Here $\deg f(x)=n$ and $\deg g(x)=m$.

By def., $f(x)\,g(x)=c_0x^0+c_1x^1+c_2x^2+......+c_kx^k$,

where $c_t=a_tb_0+a_{t-1}b_1+......+a_1b_{t-1}+b_t$.

To prove. $c_{m+n}=a_mb_n\neq 0$ and $c_i=0$ when $i>m+n$.

Now $c_{m+n}=a_{m+n}b_0+a_{m+n-1}b_1+......+a_mb_n$
$+a_{m-1}b_{n+1}+......+a_0b_{m+n}$,

where $a_m\neq 0,\ a_{m+1}=a_{m+2}=......=a_{m+n}=0$

and $b_n\neq 0,\ b_{n+1}=b_{n+2}=......=b_{m+n}=0$

$\therefore$ $c_{m+n}=a_mb_n\neq 0$.

When $i>m+n$,

then $c_i=a_ib_0+a_{i-1}b_1+......+a_{i-j}b_j+a_{i-(j+1)}b_{j+1}$
$+......+a_0b_i$

Thus c_i is the sum of the terms of the form $a_{i-j}b_j$.

But $i=(i-j)+j>m+n$.

Then either $i-j>m$ or $j>n$.

Thus one of a_{i-j} or b_j is zero in each term of the sum c_i.

$\therefore$ for $i>m+n$, c_i is the sum of zeros

$\Rightarrow$ c_i is itself a zero element.

Thus the highest non-zero co-efficient of $f(x)\,g(x)$ is $c_{m+n}=a_mb_n$.

Hence $\deg [f(x)\,.\,g(x)]=\deg f(x)+\deg g(x)$. | **C.T.M.**

Example 1. *Prove that* $R[x]$ *forms a ring, where*

$R[x]=\{f(x)/f(x)=a_0x^0+a_1x^1+......+a_nx^n\ ;\ a_i\in R\}$.

(Important)

Sol. Under Addition :

(i) Closure Axiom

To prove. $\forall f(x), g(x)\in R[x],\ f(x)+g(x)\in R[x]$

Here $f(x)=a_0x^0+a_1x^1+......+a_nx^n$

and $g(x)=b_0x^0+b_1x^1+......+b_mx^m$

Then $f(x)+g(x)=c_0x^0+c_1x^1+......+c_ix^i+......$, where $c_i=a_i+b_i$

$=\Sigma c_ix_i$

Since $a_0,\ b_0\in R$,

$\therefore$ $a_0+b_0\in R$ [$\because$ *R is a ring*]

$\Rightarrow$ $c_0\in R$; and so on.

$\therefore$ $f(x)+g(x)$ is a polynomial in x over R.

Thus $f(x)+g(x)\in R[x]$.

(ii) **Associative Law.**

To prove. $\forall\ f(x), g(x), h(x) \in R[x]$,

$[f(x)+g(x)]+h(x)=f(x)+[g(x)+h(x)]$

Let $\quad h(x)=d_0x^0+d_1x^1+\ldots\ldots+d_kx^k$

In $[f(x)+g(x)]+h(x)$,

coeff. of $x^i=(a_i+b_i)+d_i$

In $f(x)+[g(x)+h(x)]$,

coeff. of $x^i=a_i+(b_i+d_i)$

Since associative law holds in R $\quad$ [$\because$ *R is a ring*]

$\therefore \quad \forall\ a_i, b_i, d_i \in R$

$\Rightarrow \quad (a_i+b_i)+d_i=a_i+(b_i+d_i)$

$\Rightarrow$ Coeff. of x_i in $[f(x)+g(x)]+h(x)$ is the same as the coeff. of x^i in $f(x)+[g(x)+h(x)]$.

Thus $[f(x)+g(x)]+h(x)=f(x)+[g(x)+h(x)]$.

(iii) **Existence of Identity element.**

To prove. $0x^0 \in R[x]$ works as identity element of $R[x]$

i.e., $\quad \forall\ f(x) \in R[x],\ f(x)+0x^0=f(x)$.

$$\begin{aligned} f(x)+0x^0 &= a_0x^0+a_1x^1+\ldots\ldots+a_nx^n+0x^0 \\ &=(a_0+0)x^0+a_1x^1+\ldots\ldots+a_nx^n \\ &=a_0x^0+a_1x^1+\ldots\ldots+a_nx^n \\ &=f(x) \end{aligned}$$

Thus $0x^0$ works as identity element of $R[x]$.

(iv) **Existence of Inverse.**

Since R is a ring, $\quad \therefore \quad a_0 \in R \quad \Rightarrow \quad -a_0 \in R$; etc.

[$\because$ *R forms a group under addition*]

To prove. $-f(x) \in R[x]$ works as inverse of $f(x)$.

$$\begin{aligned} f(x)+[-f(x)] &= (a_0x^0+a_1x^1+\ldots\ldots+a_nx^n) \\ &\qquad +(-a_0x^0-a_1x^1\ldots\ldots-a_nx^n) \\ &=(a_0-a_0)x^0+(a_1-a_1)x^1+\ldots\ldots+(a_n-a_n)x^n \\ &=0x^0+0x^1+\ldots\ldots+0x^n \\ &=\text{zero polynomial.} \end{aligned}$$

Thus $-f(x)$ works as inverse of $f(x)$.

(v) **Commutative Law.**

To prove. $\forall\ f(x), g(x) \in R[x],\quad f(x)+g(x)=g(x)+f(x)$.

$$\begin{aligned} f(x)+g(x) &= (a_0+b_0)x^0+\ldots\ldots+(a_i+b_i)x^i+\ldots\ldots \\ &=(b_0+a_0)x^0+\ldots\ldots+(b_i+a_i)x^i+\ldots\ldots \\ &\qquad [\because\ a_0, b_0 \in R \ \Rightarrow\ a_0+b_0=b_0+a_0 ;\ etc.] \\ &=g(x)+f(x). \end{aligned}$$

Under Multiplication :

(*vi*) **Closure Axiom.**

To prove. $\forall\ f(x), g(x) \in R[x], f(x)\, g(x) \in R[x]$.

$$f(x)g(x) = a_0b_0x^0 + (a_0b_1 + a_1b_0)x^1 + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots\ldots + (a_0b_i + \ldots\ldots + a_ib_0)x^i + \ldots\ldots$$

$$= c_0x^0 + c_1x^1 + \ldots\ldots + c_ix_i + \ldots\ldots,$$

where $c_i = a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \ \ldots + a_ib_0$

$= \Sigma a_rb_s$, where $r+s=i$ and r, s are +ve integers

Now $a_i \in R,\ b_i \in R\ \forall i$

$\Rightarrow\ a_rb_s \in R$ [$\because$ *R is a ring*]

$\Rightarrow\ \Sigma a_rb_s \in R$

Thus $f(x)\, g(x) \in R[x]$.

(*vii*) **Associative Law.**

To prove. $\forall\ f(x), g(x), h(x) \in R[x]$,

$$(f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x))$$

Coeff. of x^i on L.H.S. $= \Sigma(a_r\, b_s)\, d_t$, where $r+s+t=i$

Coeff. of x^i on R.H.S. $= \Sigma a_r(b_sd_t)$, where $r+s+t=i$

Now $(a_rb_s)d_t = a_r(b_sd_t)$ [$\because$ *Associative law holds in R*]

$\therefore\ (f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x))$.

(*viii*) **Distributive Laws.**

To prove. $\forall\ f(x), g(x), h(x) \in R[x]$,

(I) $[f(x)+g(x)]h(x) = f(x)h(x) + g(x)h(x)$

(II) $h(x)[f(x)+g(x)] = h(x)f(x) + h(x)g(x)$.

On L.H.S., coeff. of $x^i = \Sigma(a_r + b_r)d_s$ ...(1),
where $r+s=i$

On R.H.S., coeff. of $x^i = \Sigma a_rd_s + \Sigma b_rd_s$ ...(2)

Since a_r, b_r, $d_s \in R$ and distributive laws hold in R,

$\therefore$ from (1), $\Sigma(a_r+b_r)d_s = \Sigma a_rd_s + \Sigma b_rd_s =$ R.H.S.

$\therefore$ Right distributive law holds in $R[x]$.

Similarly left distributive law also holds in $R[x]$.

Hence $R[x]$ forms a ring.

Example 2. *If R is a commutative ring, prove that R[x] is also a commutative ring.*

Sol. Let $f(x) = a_0x^0 + a_1x^1 + \ldots\ldots + a_mx^m$

and $g(x) = b_0x^0 + b_1x^1 + \ldots\ldots + b_nx^n$ be two elements of $R[x]$.

Then $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \ldots\ldots$

Coefficient of $x^i = a_0b_i + a_1b_{i-1} + \ldots\ldots + a_ib_0$

Similarly coefficient of x^i in $g(x)f(x)$

$$=b_0a_i+b_1a_{i-1}+\ldots\ldots+b_ia_0$$

Now R is a commutative ring [*Given*]

$\therefore\ \ a_ib_0=b_0a_i,\ a_{i-1}b_1=b_1a_{i-1}$; etc.

$\therefore$ coefficient of x^i in $f(x)g(x)$=coefficient of x^i in $g(x)f(x)$.

Thus $\quad f(x)\,g(x)=g(x)\,f(x)$

Hence R$[x]$ is also a commutative ring

Example 3. *If R has identity element, prove that R[x] has also an identity element.*

Sol. Since R has identity element, [*Given*]

$\therefore\ \exists\ 1\in R$ such that $a.1=1.a=a\quad\forall\quad a\in R$

Now $1\in R\ \Rightarrow\ 1.x^0\ R[x]$

Again $[f(x)]x^0=(a_0+a_1x+\ \ldots+a_nx^n)x^0$

$$=a_0x^0+a_1x^{1+0}+\ldots\ldots+a_nx^{n+0}$$
$$=a_0x^0+a_1x^1+\ldots\ldots+a_nx^n$$
$$=f(x)$$

Similarly $x^0[f(x)]=f(x)$.

Hence x^0 is the identity element of R$[x]$.

Example 4. *If R is an integral domain, prove that R[x] is also an integral domain.*

Sol. Let $f(x)=a_0x^0+a_1x^1+\ldots\ldots+a_mx^m\ (a_m\neq 0)$

and $\qquad g(x)=b_0x^0+b_1x^1+\ldots\ldots+b_nx^n\ (b_n\neq 0)$

be two elements of R$[x]$ such that $f(x)\neq 0$, $g(x)\neq 0$.

Since R is without zero divisors,

$$a_m\neq 0,\ b_n\neq 0\ \Rightarrow\ a_mb_n\neq 0.$$

Now $f(x)g(x)=c_0+c_1x+c_2x^2+\ldots\ldots+c_{m+n}x^{m+n}$,

where $\quad c_{m+n}=a_mb_n\neq 0$

$\therefore\qquad f(x)g(x)\neq 0$

Hence $\qquad$ R$[x]$ is without zero divisor.

Example 5. *If F is a field, prove that F[x] is an integral domain.* [Pbi. U. 1976]

Sol. Since F is a field [*Given*]

$\therefore$ F is an integral demain

$\Rightarrow$ F$[x]$ is an integral domain [*Example 4*]

LAXMI PUBLICATIONS (P) LTD